Ф А2.2.1-32-367

МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ
НАЦІОНАЛЬНИЙ ФАРМАЦЕВТИЧНИЙ УНІВЕРСИТЕТ
Факультет фармацевтичних технологій та менеджменту
Кафедра управління та забезпечення якості у фармації

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО ВПРОВАДЖЕННЯ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПРИКЛАДІ ДІЯЛЬНОСТІ НАВЧАЛЬНИХ ЗАКЛАДІВ

Виконав (ла):
здобувач вищої освіти
2 курсу, групи 1
спеціальності 073 Менеджмент
освітньої програми
Якість, стандартизація та
сертифікація
Станіслав ГОНЧАРОВ

Керівник:
доцент закладу вищої освіти
кафедри управління та забезпечення
якості у фармації
канд. фармац. наук, доц.
Тетяна ЗБОРОВСЬКА

Рецензент:
доцент закладу вищої освіти
кафедри технологій
фармацевтичних препаратів НФаУ
канд. фармац. наук, доцент
Денис ПУЛЯЄВ

Харків – 2024 рік

АНОТАЦІЯ

Станіслава ГОНЧАРОВА на тему "Розробка пропозицій щодо впровадження системи менеджменту інформаційної безпеки на прикладі діяльності навчальних закладів"

Мета дослідження: розробка заходів з впровадження системи інформаційної безпеки задля збереження конфіденційності, цілісності й доступності обігу інформації в ЗВО.

Завдання: аналіз сучасних підходів впровадження системи інформаційної безпеки; вивчення вимог стандарту ISO/IEC 27001 щодо системи забезпечення інформаційної безпеки; аналіз поточного стану діяльності ЗВО в секторі ІТ-розвитку; розробка заходів щодо впровадження системи інформаційної безпеки в ЗВО.

Об'єктом дослідження є діяльність Національного фармацевтичного університету в сфері розвитку власної ІТ-інфраструктури.

Предметом дослідження є заходи з формування системи інформаційної безпеки ЗВО.

Сформовано кроки щодо впровадження в діяльність ЗВО системи інформаційної безпеки. Запропоновано практичні дії з їх реалізації у вигляді алгоритму створення системи інформаційної безпеки.

Структура і обсяг кваліфікаційної роботи: кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, переліку посилань 30 найменувань, 3 додатків, і містить 7 рисунків, 8 таблиць. Повний обсяг магістерської роботи складає 69 сторінок, з яких перелік посилань займає 3 сторінки, додатки – 19 сторінок.

Ключові слова: система інформаційної безпеки, інформаційні ризики, заклади вищої освіти.

ABSTRACT

Stanislav GONCHAROV on the topic "Development of proposals for the implementation of the information security management system based on the example of the activities of educational institutions"

The purpose of the study: development of measures for the implementation of the information security system in order to preserve the confidentiality, integrity and availability of information circulation in higher education institutions.

Task: analysis of modern approaches to the implementation of the information security system; studying the requirements of the ISO/IEC 27001 standard regarding the information security system; analysis of the current state of activity of higher education institutions in the IT development sector; development of measures for the implementation of the information security system in higher education institutions.

The object of the study is the activity of the National Pharmaceutical University in the field of development of its own IT infrastructure.

The subject of the study is the measures to form the information security system of higher education institutions.

Steps have been taken to introduce an information security system into the activities of the ZVO. Practical actions for their implementation in the form of an algorithm for creating an information security system are proposed.

Structure and scope of the qualification work: the qualification work consists of an introduction, three sections, general conclusions, a list of references of 30 names, 3 appendices, and contains 7 figures, 8 tables. The full volume of the master's work is 69 pages, of which the list of references occupies 3 pages, appendices - 19 pages.

Keywords: information security system, information risks, higher education institutions.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ISO – International Organization for Standardization (міжнародна організація зі стандартизації)

PDCA Plan-Do-Check-Act – Цикл Шухарта-Демінга: планування – виконання запланованого – перевірка і аналіз – коригування та удосконалення

СУЯ – система управління якістю

WEF – Всесвітній економічний форум

ТЗІ – технічного захисту інформації

СУІБ – система управління інформаційною безпекою

ІБ – інформаційної безпеки

ІЕС – Міжнародною електротехнічною комісією

ПЕМВН – побічного електромагнітного випромінювання і наводів

ВЧ-нав’язування – надходження високочастотних сигналів у нелінійні (або параметричні) кола, що несуть конфіденційну інформацію

ВСТУП

Кіберзлочинність стає все більш жорстокою та витонченою, оскільки хакери розробляють новітні методи боротьби з нею. У звіті Всесвітнього економічного форуму про перспективи глобальної кібербезпеки вказується, що кількість кібератак у всьому світі зросла на 125% у 2021 році, і дані свідчать про те, що їх зростання триватиме у майбутньому. У цьому швидко мінливому ландшафті управління організаціями керівники повинні застосувати стратегічний підхід до кіберризиків та збереження власної інформації.

Щоб подолати проблеми кібербезпеки, організації повинні підвищити свою стійкість і вжити заходів щодо пом'якшення впливу кіберзагроз. Впровадження вимог стандарту ISO/IEC 27001 несе користь організації таку як:

– захист інформації в усіх формах, включаючи паперові, хмарні та цифрові дані;

– підвищення стійкості до кібератак;

– розроблену централізовано-керовану структуру, яка захищає всю інформацію в одному місці;

– захист усієї організації, зокрема від технологічних ризиків та інших загроз;

– зменшення витрат на неефективні оборонні технології;

– захист цілісності, конфіденційності та доступності даних.

Цілісний підхід описаний в ISO/IEC 27001 означає, що охопленню повинна підлягати вся організація, а не лише IT-структура. Управління людьми, технологіями та процесами – усе це приносить користь та захист [1].

Основні причини розробки та впровадження цього стандарту: конфіденційність – забезпечення доступності інформації лише для тих, хто має відповідні повноваження; доступність – забезпечення доступу до інформації лише авторизованим користувачам та в потрібний момент часу;

цілісність – забезпечення точності та повноти інформації, а також методів її обробки. Впровадження системи менеджменту інформаційної безпеки допомагає вирішити ці питання та захищає інформацію від зайвих очей, а також Система менеджменту інформаційної безпеки – інструмент для запобігання втратам підприємства.

В умовах глобалізації та розвитку ІТ-технологій захищеність інформаційних ресурсів є однією з найважливіших складових успішного розвитку суспільства. На даному етапі розвитку відбувається впровадження сучасних інформаційних технологій, що суттєво впливає на зміни у процесах управління. Але відповідно до зростання кількості та складності інформації збільшується і кількість загроз інформаційної системи загалом. Заклади вищої освіти зіграли ключову роль у розвитку комп'ютерної техніки і програмного забезпечення.

Вони розробляють, випробовують і впроваджують передові проекти в сфері ІТ. Зростання кіберзлочинності знижує захист конфіденційної інформації та розробок в навчальних закладах. Тому найбільш пріоритетним завданням в даний час є забезпечення інформаційної безпеки, успішне вирішення якого дозволить викладачам та здобувачам взаємодіяти один з одним, не турбуючись про збереження інформації [2].

В розвинених країнах світу сучасна система освіти забезпечується завдяки ефективній державній політиці регулюванню ключових процесів, розробці та реалізації дієвих стратегій розвитку та відповідному фінансуванню передбачених заходів, в тому числі й у сфері запровадження інноваційних технологій.

В Україні окресленим питанням також приділяється певна увага, проте існує потреба у запровадженні передового досвіду окремих держав світу у сфері захисту інформації в освітніх закладах. Слід наголосити, що до освітнього процесу залучаються діти та підлітки, які дуже чутливі до сприйняття будь-якої інформації, що може пропагувати шкідливі для здоров’я, психіки та безпеки даної категорії населення цінності. Поряд з цим,

потрібно забезпечити захист персональних даних здобувачів від заволодіння зловмисниками. В системі освіти також зберігається інформація про педагогічних та інші категорії працівників, навчальні матеріали у цифровому вигляді, фінансові та бухгалтерські дані, а також службова документація, приведені електронні матеріали також потребують захисту.

Для забезпечення функціонування освітніх закладів та нормальної життєдіяльності усіх учасників навчального процесу система інформаційної безпеки повинна мінімізувати ризики пошкодження баз даних, викрадення масивів конфіденційних відомостей, а також гарантувати неможливість проникнення в навчальні приміщення пропаганди, яка негативно впливає на свідомість здобувачів [3].

Мета роботи. Проаналізувавши такі тенденції розвитку діяльності вищих навчальних закладів, ми визначили за мету розробку заходів з впровадження системи інформаційної безпеки задля збереження конфіденційності, цілісності й доступності обігу інформації в ЗВО.

Об’єкт та предмет дослідження. Як об’єкт було вибрано діяльність Національного фармацевтичного університету в сфері розвитку власної IT-інфраструктури, а предметом дослідження є алгоритм формування системи інформаційної безпеки ЗВО.

Основні завдання роботи. Для досягнення визначеної мети нам необхідно здійснити:

– аналізування сучасних підходів впровадження системи інформаційної безпеки;

– вивчення вимоги стандарту ISO/IEC 27001 щодо системи забезпечення інформаційної системи;

– аналізування поточного стану діяльності ЗВО в секторі IT-розвитку;

– розробку заходів щодо впровадження системи інформаційної безпеки в ЗВО.

Методи дослідження, які ми використовуємо:

- логічний метод,
- системно-аналітичний метод,
- метод описового моделювання й узагальнення;
- метод порівняльного аналізу
- соціологічні методи.

Практичне значення отриманих результатів. Розроблено практичні рекомендації щодо впровадження системи інформаційної безпеки за вимогами стандарту ISO/IEC 27001 та створено супровідну документацію з впровадження, яка забезпечить розвиток та підтримку ІТ-сфери університету, і таким чином підвищить рівень стійкості до кіберзагроз, які можуть вплинути на імідж та стабільність роботи ЗВО.

Дослідження і публікації. Гончаров С.В., Зборовська Т. В. «Актуальність побудови інформаційної безпеки в діяльності організацій» Збірник: матер. II міжнарод. наук.-практ. internet-конференції з міжнар. участю «Актуальні проблеми якості, менеджменту і економіки у фармації і охороні здоров’я», 19 січня 2023 р., м. Харків.

Структура і обсяг кваліфікаційної роботи: кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, переліку посилань 30 найменувань, 3 додатків, і містить 7 рисунків, 8 таблиць. Повний обсяг магістерської роботи складає 69 сторінок, з яких перелік посилань займає 3 сторінки, додатки – 19 сторінок.

РОЗДІЛ 1

ІНФОРМАЦІЙНА БЕЗПЕКА В УПРАВЛІННІ ДІЯЛЬНОСТЮ СУЧАСНОЇ ОРГАНІЗАЦІЇ

1.1 Роль та місце інформаційної безпеки в інформаційному суспільстві

Інформаційна безпека є однією із важливих складових глобальної безпеки, невід'ємною умовою глобалізації та одним із факторів впливу глобальних процесів на всі сфери діяльності. Глобальний процес інформатизації суспільства, який є відображенням загальних закономірностей генезису цивілізації, сьогодні охопив усі сфери соціокультурної діяльності людини. Стрімкий розвиток і розповсюдження нових інформаційно-комунікаційних технологій обумовлює кардинальні зміни в управлінні господарськими системами різних рівнів. Формування та рівень розвитку інформації, інформаційних ресурсів та всього інформаційного простору є головною характеристикою розвитку будь-якої соціальноекономічної системи на макро- та мікрорівнях.

Особливості необмеженого і неконтрольованого впливу, несанкціонованого доступу, а також виникнення комп'ютерних вірусів та інших загроз, викликають необхідність у забезпеченні інформаційної безпеки, яка є головною частиною економічної безпеки держави та національної безпеки в цілому.

Життєдіяльність суспільства, його інформаційна безпека залежить від стабільного функціонування, живучості, надійності та готовності інформаційно-телекомунікаційних мереж.

Завдяки стрімкому технологічному прогресу постає низка життєво важливих питань щодо організації процесів оброблення, зберігання, поширення та захисту інформації в глобальних інформаційно-комунікаційних системах. Бо саме інформаційні технології та розвинена інфраструктура телекомунікацій відіграють сьогодні вирішальну роль у забезпеченні

зростання продуктивності виробництва, адміністративного і господарського управління, у розширенні інформаційної взаємодії між людьми, поширенні масової інформації, процесі інтелектуалізації суспільства.

Інформаційна безпека має важливе значення для того, щоб інформаційні технології могли відповідати очікуванням ділового світу, споживачів і урядів та щоб дійсно надавали всі ті потенційні вигоди, що їх забезпечують інформаційно-комунікаційні технології.

Складовими частинами глобальної безпеки є: національна, економічна, політична, інформаційна, технічна, фізична, соціальна, військова, екологічна, ресурсна, продовольча, енергетична, фінансово-грошова, цінова, демографічна, пожежна, медична, психологічна, психічна, кримінальна безпеки (рис. 1.1).

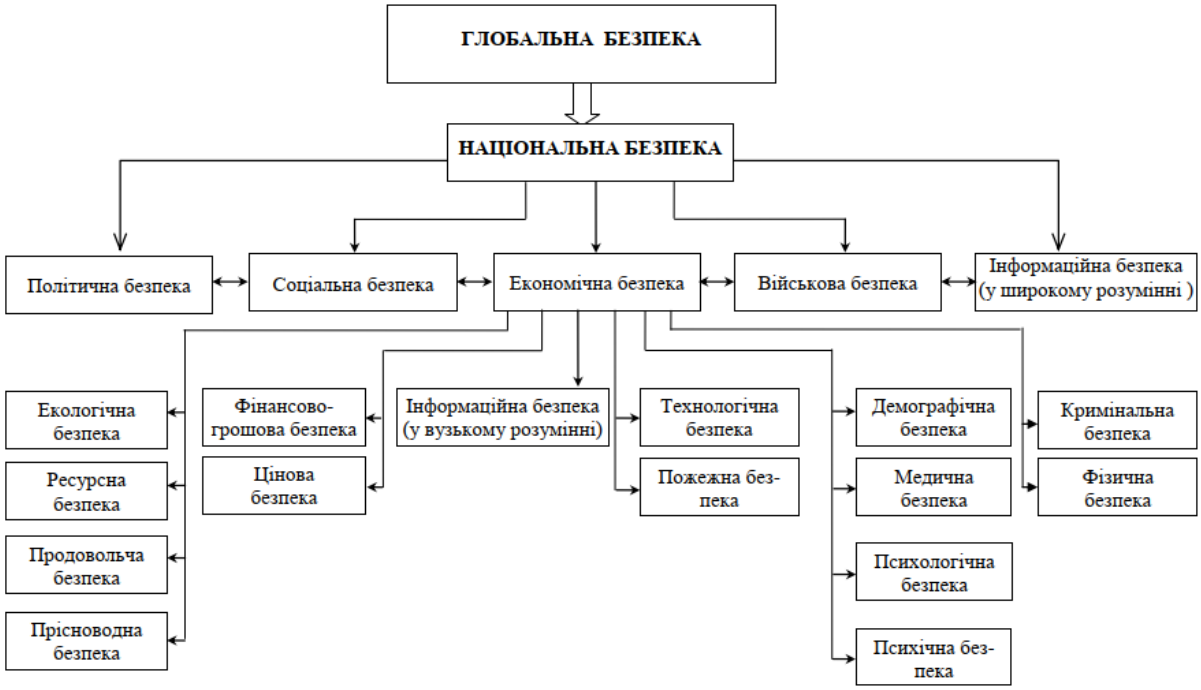

Рис. 1.1 Складові глобальної безпеки

Особливості розвитку інформації, можливості необмеженого та неконтрольованого впливу, несанкціонований доступ, комп’ютерні віруси та інше гостро поставили перед суспільством проблеми інформаційної безпеки.

Інформаційна безпека повинна здійснюватися комплексно та систематично з використанням повного набору засобів (організаційних,

технічних, апаратнопрограмних та ін.) щоб запобігти інформаційному тиску та в цілому будь-якій іншій небезпеці.

Інформаційна безпека є більш вузьким поняттям і розглядається як складова національної безпеки. Інформаційна безпека містить у собі захист інформаційних мереж, ресурсів, програмних засобів, об'єктів інтелектуальної власності й інших нематеріальних активів, включаючи майнові інтереси учасників підприємницької діяльності.

В умовах глобалізації посилюється значимість проблем, які пов’язані з інформаційною безпекою, а саме:

– виникнення та зростання кіберзлочинності та кібертероризму;

– виникнення окремих видів інформаційної зброї та ведення глобальних інформаційних війн;

– втрата національної культури або злиття її з іншими, вплив культур країн світу та менталітету інших націй;

– стимулювання інформаційно-розвиненими державами «відпливу інтелекту» та капіталів;

– виникнення явищ «інформаційного вибуху», «інформаційного голоду» та «інформаційних війн»;

– ускладнення вирішення питань збереження державної, комерційної, службової та персональної таємниці, тому що низький рівень вітчизняних інформаційних технологій обумовив побудову інформаційної інфраструктури України на базі імпортної техніки й технології;

– розвиток телебіометрики й сенсорних мереж у взаємодії людей між собою та навколишнім середовищем.

Інформаційна безпека не може бути вирішена без впровадження нових ідей, нових знань, нової політики у сфері інформатизації. Тенденції розвитку сучасного світу характеризуються створенням єдиного глобального інформаційного простору на планеті, отже, проблема інформаційної безпеки стає проблемою колективною, а не окремо взятої країни.

1.2 Стан кібербезпеки та заходи у сфері інформаційної безпеки

Пандемія коронавірусу прискорила використання цифрових інструментів у бізнесі та вдома. Це, в свою чергу, призвело до того, що кіберінциденти стали частішими, найдорожчими та руйнівними. Один із найважливіших висновків, які було зроблено бізнесом – необхідність переходити від кібербезпеки до кіберстійкості.

Під час пандемії COVID-19 цифровізація прискорилася в рази. Наприклад, стали при виконанні професійної діяльності використовувати у 10 разів частіше відеоконференцій. Логічно, що зі зростанням використання цифрових інструментів зростає й обсяг створюваних даних. За оцінками Світового банку в 2022 році щорічний загальний обсяг інтернет-трафіку збільшився приблизно на 50% порівняно з рівнем 2020 року та сягає 4,8 зеттабайт. Пандемія також яскраво показала, як тісно взаємопов’язані всі підприємства між собою і як зростання цифровізації вивело населення планети на новий рівень кіберзагроз та атак. У 2021 році відбулися неодноразові порушення критичної інфраструктури та безліч атак на ланцюжки поставок. Це дало зрозуміти, як кібербезпека однієї компанії може мати каскадний ефект на багато інших, від прямих клієнтів до кінцевих споживачів.

Враховуючи ці безперервні кіберпроблеми, Центр кібербезпеки Всесвітнього економічного форуму (WEF) опублікував звіт «Глобальні перспективи кібербезпеки до 2022 року», в якому містяться прогнози та критичні висновки, отримані від більш ніж 120 світових кіберлідерів.

Дослідження WEF виявило три основні розриви у сприйнятті між керівниками, орієнтованими на безпеку (наприклад, головним спеціалістом з інформаційної безпеки), та керівниками бізнесу (наприклад, генеральним директором). Ці розбіжності найбільш помітні у наступних сферах діяльності організацій:

1. Пріоритетність кіберрішень у бізнесі. 92% опитаних керівників бізнесу погоджуються з тим, що кіберстійкість інтегрована у стратегії

управління ризиками підприємства, проте лише 55% опитаних керівників, орієнтованих на безпеку, погоджуються з цим твердженням.

2. Підтримка керівництва у сфері кібербезпеки. 84% респондентів стверджують, що кіберстійкість вважається пріоритетом бізнесу в їхній організації за підтримки з боку керівництва, проте менша кількість опитаних (68%) розглядають кіберстійкість як основну частину загального управління ризиками. Внаслідок такої невідповідності багато керівників служб безпеки, як і раніше, зазначають, що з ними не радяться при прийнятті бізнес-рішень, що може ускладнити виявлення та пом'якшення ризиків безпеки та призвести до прийняття менш безпечних рішень. У багатьох організаціях кібербезпека все ще пасе задніх.

3. Пошук та утримання талановитих фахівців з кібербезпеки. Дослідження WEF показало, що 59% усіх респондентів вважають складним адекватно реагувати на інцидент кібербезпеки через брак кваліфікованих фахівців у їхній команді. Хоча більшість респондентів назвали підбір та утримання талантів найскладнішим завданням керівники компаній, схоже, не так гостро усвідомлюють ці проблеми, як їхні колеги з питань безпеки. Вони вважають, що їхня здатність відреагувати на атаку за допомогою персоналу є однією з їхніх головних вразливостей.

4. Постійно зростаюча загроза програм-вимагачів. Опитування підтверджує, що ransomware-атаки перебувають у центрі уваги кіберлідерів. Понад 50% респондентів відзначили, що здирництво є однією з найбільших проблем, коли мова заходить про кіберзагрози. Крім того, 80% підкреслили, що такий вид атак є небезпечною і зростаючою загрозою для громадської безпеки. Вони частішають та стають більш витонченими, за ними йдуть атаки з використанням соціальної інженерії, які посідають друге місце за ступенем занепокоєння кіберлідерів.

5. Зловмисна діяльність інсайдерів. Шкідливий інсайдер – це один із нинішніх чи колишніх співробітників організації, підрядників або довірених

ділових партнерів, який зловживає своїм авторизованим доступом до критичних активів.

Хоча існує безліч факторів, що впливають на політику кібербезпеки, більшість респондентів (81%) відзначили, що цифрова трансформація є основним фактором підвищення кіберстійкості. Великий відсоток (87%) керівників планують підвищити кіберстійкість шляхом зміцнення політик, процесів та стандартів із залучення та управління третіми сторонами.

Дослідження WEF показують, що кіберстійкість малого та середнього бізнесу розглядається як критична загроза для ланцюжків поставок, партнерських мереж та систем. У дослідженні 88% респондентів вказали, що вони стурбовані кіберстійкістю бізнесу у своїй екосистемі. Крім того, майже половина (48%) респондентів вважають, що автоматизація та машинне навчання призведуть до найбільших змін у кібербезпеці в найближчі два роки. Справді, ці технологічні розробки напевно посилять вже існуючий дисбаланс між атакуючими та захисниками.

Хоча кібератаки не припиняться найближчим часом, і поки не знайдено чарівної пігулки, яка здатна вирішити всі проблеми кібербезпеки, існують чіткі та конкретні кроки, які керівники можуть зробити, щоб найкращим чином підготувати себе та свої організації до атаки. Кібербезпека – це безперервний процес. Перехід від кібербезпеки до кіберстійкості є важливим кроком на шляху до більш надійного та стійкого майбутнього.

Значна цифровізація відкрила шлях для взаємодії та зв’язку у той час, коли світ мав залишатися розділеним. Її переваги є очевидними, але також очевидними є і загрози. Щоб забезпечити надійне, безпечне та захищене цифрове середовище, необхідно, щоб керівники краще впроваджували кібербезпеку та долали ізольованість як усередині організацій, так і між ними для підвищення кіберстійкості [4].

1.3 Джерела загроз та засоби їх впливу на об’єкти інформаційної безпеки

Джерела загроз інформаційній безпеці можна поділити на зовнішні і внутрішні [5]. До зовнішніх джерел відносяться:

– недружня політика іноземної держави в області глобального інформаційного моніторингу, поширення інформації і нових інформаційних технологій;

– діяльність іноземних розвідувальних і спеціальних служб;

– діяльність іноземних політичних і економічних структур, спрямована проти інтересів держави; злочинні дії міжнародних груп, формувань і окремих осіб;

– стихійні лиха і катастрофи.

До внутрішніх джерел відносяться:

– протизаконна діяльність політичних і економічних структур в області формування, поширення і використання інформації;

– неправомірні дії державних структур, що приводять до порушення законних прав громадян і організацій в інформаційній сфері;

– порушення установлених регламентів збирання, оброблення і передавання інформації; навмисні дії і неумисні помилки персоналу інформаційних систем;

– відмови технічних засобів і збої програмного забезпечення в інформаційних і телекомунікаційних системах.

Засоби дії загроз на об’єкти інформаційної безпеки поділяються на інформаційні, програмно-математичні, фізичні, радіоелектронні, організаційноправові.

До інформаційних засобів відносяться:

– порушення адресності і своєчасності інформаційного обміну, протизаконне збирання і використання інформації;

– несанкціонований доступ до інформаційних ресурсів;

– маніпулювання інформацією (дезінформація, приховання або спотворення інформації);

– незаконне копіювання даних в інформаційних системах;

– використання засобів масової інформації з позицій, що суперечать інтересам громадян, організацій і держав, розкрадання інформації з бібліотек, архівів, банків і баз даних; порушення технології оброблення інформації.

Програмно-математичні засоби включають:

– впровадження програм-вірусів;

– установку програмних і апаратних закладних пристроїв;

– знищення або модифікацію даних в інформаційних системах.

Фізичні засоби включають:

– знищення або руйнування засобів оброблення інформації і зв’язку; знищення, руйнування або розкрадання машинних або інших оригіналів носіїв інформації;

– розкрадання програмних або апаратних ключів і засобів криптографічного захисту інформації;

– дія на персонал; постачання «заражених» компонентів інформаційних систем.

Радіоелектронними засобами є:

– перехоплення інформації в технічних каналах її витоку;

– впровадження електронних пристроїв перехоплення інформації в технічних засобах і приміщеннях;

– перехоплення, дешифровка і нав’язування помилкової інформації в мережах передачі даних і лініях зв’язку;

– дія на парольно-ключові системи; радіоелектронне придушення ліній зв’язку і систем управління.

Організаційно-правові засоби включають:

– закупівлю недосконалих або застарілих інформаційних технологій і засобів інформатизації;

– невиконання вимог законодавства і затримки в прийнятті необхідних нормативно-правових положень в інформаційній сфері;

– неправомірне обмеження доступу до документів, що містять важливу для громадян і організацій інформацію.

У результаті дії загроз інформаційній безпеці може бути завдано серйозного збитку життєво важливим інтересам України в політичній, економічній, оборонній та інших сферах діяльності держави, заподіяний соціально-економічний збиток суспільству й окремим громадянам.

Загрози інформаційній безпеці можуть завдавати фізичного, матеріального і морального збитку громадянам, викликати неадекватну соціальну або кримінальну поведінку груп людей або окремих осіб, здійснити вплив на процеси освіти і формування особи.

З метою запобігання, відбивання і нейтралізації загроз інформаційній безпеці застосовуються базові методи. До них відносяться правові, програмно-технічні й організаційно-економічні методи [5].

1.4 Етапи розвитку нормативної бази у сфері інформаційної безпеки.

Розвиток телекомунікаційних мереж проходить на фоні підвищення вимог з боку користувачів та держави до інформаційної безпеки поряд з вимогами до надійності функціонування зв’язку, сталості телекомунікаційних мереж та якості телекомунікаційних послуг. Зростає потреба у безпечних інформаційно-телекомунікаційних системах для забезпечення інформаційно-аналітичної діяльності державних установ та установ усіх форм власності, ефективного функціонування електронної інформаційної системи «Електронний уряд», систем електронно-цифрового підпису, електронного документообігу.

Інформаційна безпека та сталість телекомунікаційних мереж є частиною задач захисту інформаційного простору України та державної політики у сфері зв'язку щодо забезпечення оборони, національної безпеки, охорони правопорядку. Основи державної політики щодо безпеки України в інформаційній сфері визначені основоположним Законом «Про основи національної безпеки України» (від 19.06.2003 № 964-IV). Закон визначає основні засади гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз національним інтересам і національній безпеці України в усіх сферах життєдіяльності [6].

Розробляється низка нормативно-правових актів у сфері інформаційної безпеки та захисту інформаційно-телекомунікаційних систем. Інформаційна безпека телекомунікаційних мереж, як складова інформаційно-телекомунікаційних мереж, стала важливою техніко-економічною й політичною проблемою.

Розвиток нормативно-правової бази стосовно інформаційної безпеки інформаційно-телекомунікаційних систем можна поділити на декілька етапів. Перший етап започатковано в 1992 – 1996 рр. Законами України «Про інформацію» (від 02.10.92 р), «Про державну таємницю» (від 21.01.94 р.), «Про науково-технічну інформацію» (від 25.06.93 р.). Перший етап завершується стандартизацією положень технічного захисту інформації в ДСТУ 3396.0-96, ДСТУ 3396.1-96, ДСТУ 3396.2-97.

Другий етап розвитку нормативно-правової бази розпочатий затвердженням Кабінетом Міністрів України 8 жовтня 1997 р. постанови № 1126 про «Концепцію технічного захисту України». Згідно з цими концепціями в Україні започатковується система технічного захисту інформації (ТЗІ) і на підприємствах будь-якої форми власності утворюються підрозділи ТЗІ. У цей самий період почала активно діяти низка підприємств із виготовлення засобів захисту інформації, захищених комп'ютерів («Плутон», «Плазма-3В», ЕОМ-П тощо), програмно-апаратних комплексів

захисту інформації від несанкціонованого доступу («Гриф», «Інспектор», «АІС» тощо).

Третій етап розвитку нормативно-правової бази ініційований низкою Указів Президента України «Про заходи щодо розвитку національної складової глобальної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31.07.2000 р. № 928 і вінчається постановою Кабінету Міністрів України № 208 від 24 лютого 2003 р. «Про заходи щодо створення електронної інформаційної системи «Електронний Уряд». Характерним для цього періоду є розширення об'єкта захисту – захисту підлягає не тільки державна таємниця і конфіденційна інформація, що належить державі, а й відкрита інформація. Протягом третього етапу введені в дію нормативні документи щодо вимог до захисту інформації в локальних обчислювальних мережах і в Інтернет [7, 8]. Характерним є все більший наголос на захисті відкритої інформації. Для розв'язання завдань захисту інформації в інфокомунікаціях України стали актуальними також рекомендації ITU X.800 «Архітектура безпеки ВВС», ISO/SEC 10181 «Основні положення безпеки відкритих систем» [9, 10].

Теоретичні положення і теореми щодо інформаційної безпеки є досить складними, а деякі з них залишаються засекреченими. Тому результати теоретичних досліджень і аналізу практики побудови систем інформаційної безпеки прийнято викладати у вигляді стандартів. Стандарти містять основні практичні правила, вичерпний набір засобів управління інформаційною безпекою та процедури забезпечення інформаційної безпеки. Стосовно управління інформаційною безпекою найбільш відомим є британський стандарт BS 7799 «Практичні правила управління інформаційною безпекою». Стандарт розроблений як керівництво і рекомендації. Набір засобів управління безпекою заснований на реальних заходах захисту інформації. Розширення сфери дії інформаційних технологій потребує перегляду підходів до інформаційної безпеки. Загальні принципи побудови й експлуатації безпечних інформаційних технологій окреслюються за допомогою базової

технічної моделі забезпечення безпеки інформаційних технологій (позначається як модель ІТ-безпеки). Така модель впроваджується міжнародним стандартом ISO/IEC 15408 «Єдині критерії оцінювання безпеки інформаційних технологій» і визначає принципово нову технологію створення систем ІТ-безпеки на підставі розробляння профілю захисту та проекту безпеки.

Четвертий етап розвитку нормативно-правової бази ознаменувався прийняттям Закону «Про телекомунікації». Інформаційна безпека телекомунікаційних мереж визначається законом як здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації. Закон «Про телекомунікації» визначає основні ключові завдання інформаційної безпеки телекомунікаційних мереж, основні засоби їх виконання та відповідальність суб'єктів інформаційних відносин щодо забезпечення інформаційної безпеки [11].

П'ятий етап – є етапом розвитку нормативно-правової бази захисту інформаційних ресурсів в усіх видах державної, комерційної та персональної інформації в інформаційно-телекомунікаційних системах та інформаційному просторі України. Серед інфраструктури комунікацій телекомунікаційні мережі є найбільш критично важливими для безпеки суспільства та держави. Інформаційній безпеці інформаційно-телекомунікаційних мереж в Україні приділяється все більша увага. Термін «автоматизована система» замінюється на термін «інформаційно-телекомунікаційна система». На даному етапі вступають в дію Закон та Правила забезпечення захисту інформації в інформаційно-телекомунікаційних системах, а також Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Низка важливих міжнародних стандартів прийняті як державні стандарти України методом обкладинки [12-15]. Тобто ці міжнародні стандарти переведені

українською мовою і введені як обов’язкові для виконання на території України. Їх впровадження дає змогу бізнесу отримувати міжнародні сертифікати на побудовані системи інформаційної безпеки.

1.5 Розроблені стандарти інформаційної безпеки для захисту підприємств

Так, перші напрацювання в цій сфері були наслідком роботи окремих національних та міжнародних форумів, зокрема, Стенфордських консорціумів з досліджень питань інформаційної безпеки та політики у 1990-х роках. На сучасному етапі розробкою міжнародних стандартів займаються Міжнародна організація з стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC). В області інформаційних технологій, ISO і IEC організований спільний технічний комітет, ISO/IEC JTC1, основним завданням якого є підготовка Міжнародних стандартів інформаційної безпеки.

Розроблені стандарти є керівними положеннями під час забезпечення захисту інформації в кіберпросторі. Таким чином, система кібербезпеки, яка базується на міжнародних стандартах інформаційної безпеки, надзвичайно важлива у сучасному цифровому світі, а система управління інформаційною безпекою (СУІБ) є однією з основних категорій цієї сфери. Так, СУІБ становить собою частину загальної системи управління, яка ґрунтується на підході, що враховує бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки (ІБ) [16]. Остання включає в себе три основні компоненти: конфіденційність, можливість застосування і цілісність.

Сімейство міжнародних стандартів управління безпекою 2700х активно розвивається та призначене для забезпечення ІБ організації. Крім того, воно включає стандарти, що визначають вимоги до СУІБ, систему управління ризиками, метрики і вимірювання ефективності механізмів контролю, а також керівництво з впровадження.

Стандарти СУІБ включають стандарти, які: визначають вимоги до СУІБ, а також до тих, хто сертифікує такі системи; забезпечують безпосередню підтримку, містять докладні рекомендації і/або інтерпретацію загального процесу розробки, впровадження, забезпечення працездатності та поліпшення СУІБ; містять керівництва по СУІБ для конкретних галузей; містять вказівки з оцінки відповідності для СУІБ. Водночас терміни та визначення, що використовуються в цій стандартизації, включають в себе найбільш використовувані в сімействі стандартів СМІБ терміни та визначення; не містять всіх термінів і визначень, що застосовуються в стандартах СУІБ; не обмежують сімейство стандартів на СУІБ у визначенні нових термінів [17].

Міжнародна стандартизація в галузі ІБ охоплює стандарти, котрі умовно поділяються на 4 групи:

– стандарти для огляду і введення в термінологію;

– стандарти, які визначають обов’язкові вимоги до СУІБ (система управління інформаційною безпекою);

– стандарти, що визначають вимоги і рекомендації для аудиту СУІБ;

– стандарти, що пропонують кращі практики впровадження, розвитку та вдосконалення СУІБ.

Так, до стандартів для огляду і введення в термінологію входить стандарт ISO/IEC 27000 «Інформаційні технології – Методи і засоби забезпечення безпеки – Система менеджменту інформаційної безпеки – Загальні відомості та словник», що містить загальні відомості про систему менеджменту ІБ та включає тлумачення відповідної термінології [18].

Стандарти, які визначають обов’язкові вимоги до СУІБ, включають в себе ряд стандартів: ISO/IEC 27001 «Інформаційна технологія – Методи забезпечення безпеки – Системи менеджменту інформаційної безпеки – Вимоги», що зібрав описи найкращих світових практик в області управління інформаційною безпекою. Цей стандарт визначає вимоги до проектування,

впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою з урахуванням обставин організації, а також містить вимоги для оцінювання та оброблення ризиків інформаційної безпеки, пов'язаних з потребами організації. Вимоги, наведені в ISO/IEC 27001, є загальними та можуть бути запроваджені для всіх організацій незалежно від типу, розміру та природи [19]. Крім того, документ встановлює вимоги до системи менеджменту інформаційної безпеки для демонстрації здатності організації захищати свої інформаційні ресурси. Цей стандарт підготовлений як модель для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та поліпшення системи менеджменту інформаційної безпеки [20].

Щодо стандартів, що визначають вимоги і рекомендації для аудиту СУІБ, то до них належать: ISO/IEC 27006 «Інформаційні технології – Методи забезпечення безпеки – Вимоги до органів аудиту і сертифікації систем управління інформаційною безпекою», що розширює вимоги стандарту ISO 17021 спеціально для органів, які проводять аудит і сертифікацію СУІБ; ISO/IEC 27007 «Інформаційні технології – Методи забезпечення безпеки – Керівництво по аудиту – Систем менеджменту інформаційної безпеки», що пропонує рекомендації з проведення аудитів СУІБ з боку сертифікаційних організацій. Він корисний для аудиторів цих організацій; ISO/IEC TR 27008 «Інформаційні технології – Методи забезпечення безпеки – Керівництво для аудиторів щодо механізмів контролю СУІБ», що є додатковим стандартом до ISO 19011: 2011спеціально для СУІБ. Він спеціалізований для аудиту коштів управління інформаційною безпекою в організації.

Найбільш об'ємною є група стандартів, що пропонують кращі практики впровадження, та вдосконалення СУІБ, до якої входять: ISO/IEC 27002 «Інформаційні технології – Методи забезпечення безпеки – Практичні правила управління інформаційною безпекою. Друга редакція 01.10.2013», що є найпопулярнішим стандартом групи після ISO 27001 та надає відмінні вказівки для розробки, впровадження, підтримки і вдосконалення СУІБ. Так,

цей міжнародний стандарт розроблено для організацій для використання як довідкової інформації щодо вибору заходів безпеки під час впровадження СУІБ на базі ISO/IEC 27001 або як настанову для організацій, які впроваджують загальноприйняті заходи інформаційної безпеки. Цей стандарт також призначено для використання в розробленні установчих документів з управління інформаційною безпекою, специфічних для промисловості та організацій, з урахуванням специфічних ризиків інформаційної безпеки їх середовища.

Організації всіх типів та розмірів (охоплюючи публічний та приватний сектор, комерційні та неприбуткові) збирають, обробляють, зберігають та передають інформацію в багатьох формах, включаючи електронну, фізичну та усну (наприклад, бесіди та презентації) [21]. ISO/IEC 27003 «Інформаційні технології – Методи забезпечення безпеки – Керівництво по впровадженню системи управління інформаційною безпекою», що дає вказівки і методику для процесів розробки і впровадження СУІБ. Метою зазначеного стандарту є надання допомоги під час реалізації СУІБ у межах організації відповідно до ISO/IEC 27001. Варто зазначити, що у стандарті приведені рекомендації та роз’яснення, однак не визначено жодних вимог. Водночас ISO/IEC 27003 визначає фази планування проекту СУІБ та: призначений для використання у корпоративних системах, що впроваджують СУІБ; застосовується організаціями всіх типів і розмірів; фокусується на критичних аспектах, необхідних для успішного проектування та впровадження СУІБ; описує процес специфікації та проектування СУІБ з моменту початку проектування до подання планів впровадження системи; описує процес отримання затвердження з боку керівництва впровадження СУІБ; визначає проект впровадження СУІБ; забезпечує керівництво планом проекту СУІБ.

Застосування міжнародного стандарту ISO/IEC 27003 дозволить: оптимізувати вартість побудови та підтримання ІБ; постійно відслідковувати та оцінювати ризики з урахуванням цілей бізнесу; ефективно виявляти найбільш критичні ризики та знижати ймовірність їх реалізації; розробити

ефективну політику ІБ; ефективно розробляти, впроваджувати та тестувати плани відновлення бізнесу; забезпечити розуміння питань ІБ керівництвом та всіма працівниками підприємства, де впроваджується СУІБ; забезпечити підвищення репутації та ринкової привабливості підприємств. ISO/IEC 27004 «Інформаційні технології – Методи забезпечення безпеки – Системи менеджменту інформаційної безпеки – Вимірювання», що є керівництвом для вибору, проектування, управління і поліпшення засобів і методів вимірювання ефективності та результативності системи. Цей Міжнародний стандарт надає вказівки щодо розробки та використання заходів та вимірювань з метою оцінки ефективності впровадженої СУІБ та елементів управління або груп контролю, визначених у ISO/IEC 27001. Так, документ включає політику, управління ризиками інформаційної безпеки, цілі контролю, контроль, процеси та процедури, підтримку процесу її перегляду, допомогу у визначенні чи потрібно змінювати або вдосконалювати будь-який із процесів чи Право та державне управління контроль СУІБ.

Варто пам’ятати, що жодне вимірювання контролю не може гарантувати повну безпеку. Реалізація цього підходу є програмою вимірювання інформаційної безпеки, яка допоможе керівництву у виявленні та оцінці невідповідних і неефективних процесів та засобів управління СУІБ та визначення пріоритетності дій, пов’язаних із вдосконаленням чи зміною цих процесів та/або контролю. Він також може допомогти в організації демонстрації відповідності ISO/IEC 27001 та надати додаткові докази для огляду керівництва та процесів управління ризиками інформаційної безпеки [22]. ISO/IEC 27005 «Інформаційні технології – Методи забезпечення безпеки – Управління ризиками інформаційної безпеки», що є одним з найважливіших в групі. Незважаючи на те, що це тільки рекомендаційний, а не обов’язковий стандарт, його призначення полягає в тому, що управління ризиками – один з найважливіших процесів для інформаційної безпеки. Цей стандарт надає рекомендації щодо управління ризиками інформаційної безпеки в організації, зокрема, підтримуючи вимоги СУІБ відповідно до

ISO/IEC 27001. Однак цей Міжнародний стандарт не передбачає конкретних методів управління ризиками ІБ. Організація повинна визначити свій підхід до управління ризиками, залежно, наприклад, від сфери застосування СУІБ, контексту управління ризиками чи галузевого сектору [23].

ISO/IEC 27011 «Інформаційні технології – Методи забезпечення безпеки – Керівництво з управління інформаційною безпекою для телекомунікацій ISO / IEC 27002», що є спеціалізованим керівництвом по СУІБ в телекомунікаційних організаціях. Суміжним до ISO/IEC 27011 є стандарт ISO/IEC 27031 «Інформаційні технології – Методи забезпечення безпеки – Керівництво по забезпеченню готовності інформаційних і комунікаційних технологій до їх використання для управління безперервністю бізнесу», що є стандартом-керівництвом щодо забезпечення безперервності бізнесу в інформаційних комунікаційних технологіях (ІКТ) та впровадження плану готовності послуг ІКТ, який забезпечить безперервність бізнесу під час збоїв.

Так, у стандарті описані принципи забезпечення готовності ІКТ. У ньому наводяться основні методи і процедури визначення та опису всіх аспектів, таких як критерії ефективності, проектування та впровадження, що впливають на готовність ІКТ організації. Він також пропонує узгоджений і загальноприйнятий підхід до вимірювання характеристик, відповідних програмі забезпечення готовності ІКТ до забезпечення безперервності бізнесу. Даний стандарт поширюється на всі події та інциденти (включаючи пов’язані з безпекою), які впливають на інфраструктуру і системи ІКТ. Він включає і доповнює практику обробки інцидентів в області інформаційної безпеки і управління ними, а також планування готовності і сервіси ІКТ [24].

Також, з точки зору практичних рекомендацій щодо забезпечення аварійного відновлення ІКТ, доволі цікавим є стандарт ISO/IEC 24762 «Інформаційні технології – Методи забезпечення захисту – Рекомендації по послугам для аварійного відновлення інформаційних і комунікаційних технологій». ISO/IEC 27033, що замінює відомий міжнародний стандарт

мережевої безпеки ISO 18028. Так, стандарт включає в себе декілька частин, з яких найбільш вагомими є ISO/IEC 27033-1 «Інформаційні технології – Методи забезпечення безпеки – Мережева безпека – Основні концепції управління мережевою безпекою», що є першим з групи спеціалізованих стандартів в галузі забезпечення інформаційної безпеки мережевої інфраструктури; та ISO / IEC 27033-3 «Інформаційні технології – Методи забезпечення безпеки – Мережева безпека – Базові мережеві сценарії – загрози, методи проектування та механізми контролю», що має практичне значення [25]. ISO/IEC 27034-1 «Інформаційні технології – Методи забезпечення безпеки – Огляд та основні концепції в області забезпечення безпеки додатків», що є першим з іншої групи спеціалізованих стандартів в галузі забезпечення інформаційної 2019 р., безпеки прикладного програмного забезпечення. ISO/IEC 27035 «Інформаційні технології – Методи забезпечення безпеки – Управління інцидентами безпеки», що є одним з цінних стандартів в групі з практичною вартістю в галузі управління інцидентами з ІБ, адже стандарт є рекомендацією щодо виявлення, реєстрації та оцінки інформації, випадків порушення безпеки і уразливості. Стандарт допомагає організації реагувати на інциденти порушення безпеки, включаючи відповідні заходи контролю для запобігання та скорочення, відновлення наслідків, і таким чином, вчитися і вдосконалювати свій загальний підхід.

Крім того, стандарт може бути застосований до будь-якої організації, незалежно від розміру. Він охоплює діапазон інцидентів інформаційної безпеки, незалежно від того, чи є вони навмисними або аварійними, спричинені через технічні чи фізичні засоби Інтеграція інцидентів ІБ системи управління має ряд переваг, зокрема: підвищення загальної інформаційної безпеки; зменшення негативного впливу на бізнес; зміцнення інцидентів ІБ, профілактика, визначення пріоритетів, докази; сприяння бюджетному і ресурсному обґрунтуванню; поліпшення оновлення інформаційної безпеки оцінки ризиків та управління результатами; забезпечення підвищення

інформованості в безпеці інформації та матеріалів, навчальна програма; забезпечення взаємозв'язку інформаційної політики безпеки і загальної документації [26].

Перевагами застосування Міжнародних стандартів ISO 27000х є: забезпечення безперервності, мінімізація ризиків, забезпечення комплексного та централізованого контролю рівня захисту інформації, забезпечення цілісності, конфіденційності та доступності критичних інформаційних ресурсів інформаційно-комунікаційних систем та мереж, зниження витрат на інформаційну безпеку. Окрім зазначених стандартів, до системи міжнародної стандартизації ІБ входить безліч документів, що містять рекомендації та вимоги до впровадження та функціонування СУІБ, які слугують основою для розроблення та прийняття внутрішньодержавних правил та інструкцій.

Таким чином, стандарти серії ISO/IEC 27000 дійсно допомагають зробити безпечнішими усі сфери інформаційного життя, захищаючи приватність, фінанси, індивідуальну або корпоративну репутацію, при цьому постійно розвиваючись і вдосконалюючись [27].

Висновки до розділу 1

В розділі автором зроблено аналіз джерела літератури та Internet ресурсів та встановлено підходи до кіберзахисту вцілому. Вивчено нормативно-правові засади інформаційного захисту в Україні та світі.

Автором проведено аналіз категорій ризиків інформаційної системи держави та організацій, їх можливі наслідки та впливи на всіх учасників суспільства.

Також автор дослідив та встановив ключові аспекти впровадження на підприємстві системи інформаційного захисту, які зазначено та рекомендовано в міжнародному сімействі стандартів управління безпекою.

РОЗДІЛ 2

АНАЛІЗ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА

2.1 Складові інформаційної безпеки підприємства

Діяльність суб'єктів господарювання в умовах становлення ринкових відносин потребує швидкого виявлення факторів, які обумовлюють інформаційну безпеку підприємства та адаптації останнього до динаміки зовнішнього середовища шляхом усунення виниклих загроз. Ринкова економіка, як відомо, ґрунтується на засадах конкуренції між учасниками ринку, що є постійним джерелом ризику.

Таким чином, управління інформаційною безпекою можна розглядати як невід'ємну частину системи управління підприємством, спрямованого на протидію зовнішнім і внутрішнім загрозам його функціонуванню. Здійснення заходів щодо забезпечення інформаційної безпеки підприємства необхідне для захищеності його діяльності від негативних впливів зовнішнього середовища і підтримки стану найефективнішого використання всіх видів ресурсів з метою запобігання загрозам і забезпечення стійкості та стабільного функціонування підприємства у поточний час і на перспективу.

Наведемо загальну схему головних складових інформаційної безпеки підприємства (рис. 2.1).

Складові інформаційної безпеки підприємства – це сукупність основних напрямів його інформаційної безпеки, суттєво відмінних один від одного за своїм змістом. Розглянемо детально кожну зі складових інформаційної безпеки.

1. Технічна складова. Найбільш дослідженою та головною в усій сукупності складових інформаційної безпеки є технічна, яка в свою чергу складається з засобів захисту та каналів витоку.

Вся сукупність технічних засобів захисту поділяється на фізичні, програмно-технічні та апаратні і включає в себе електричні, механічні, електромеханічні та електронні пристрої. Фізичні засоби реалізуються у

вигляді автономних пристроїв та систем, що виконують функції загального захисту об’єктів, на яких обробляється інформація. Програмно-технічні засоби є програмним забезпеченням, що виконує функції захисту інформації.

Апаратні засоби розміщують безпосередньо в обчислювальній техніці, в телекомунікаційній апаратурі або в пристроях, що пов’язані з подібною апаратурою за допомогою стандартного інтерфейсу.

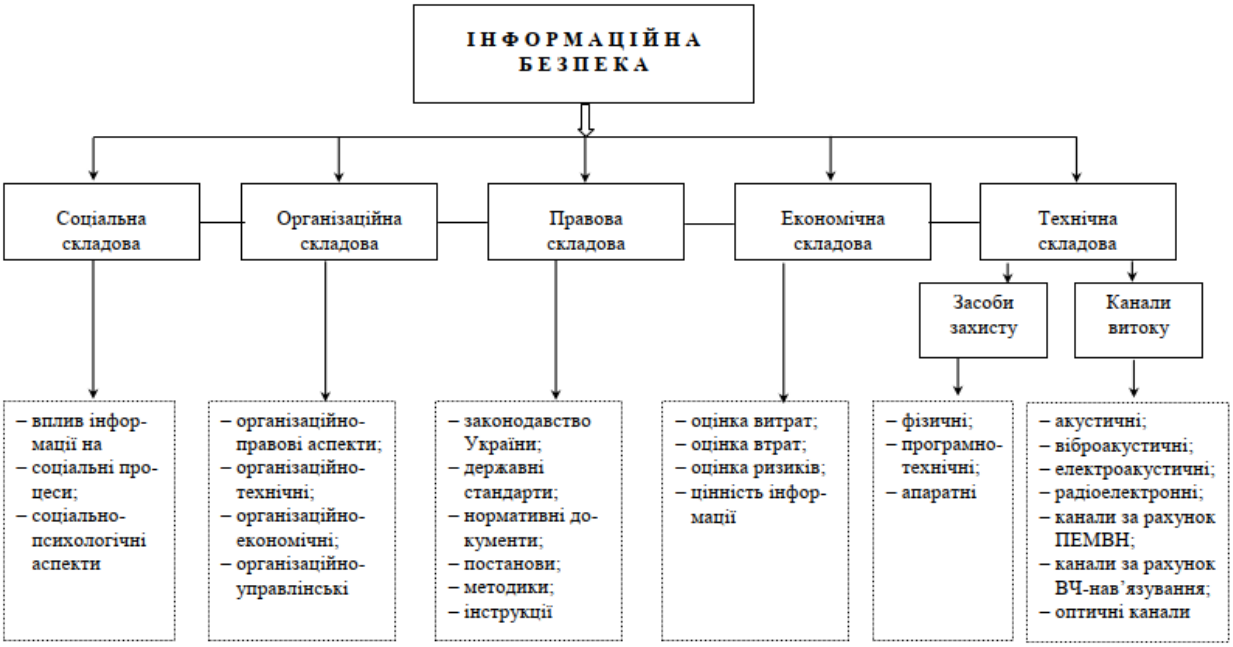

Рис. 2.1 Складові інформаційної безпеки підприємства

Канали витоку інформації у свою чергу підрозділяються на акустичні, віброакустичні, електроакустичні, радіоелектронні, канали за рахунок ПЕМВН, канали за рахунок ВЧ-нав’язування та оптичні канали.

2. Правова складова. До правової складової відноситься законодавство України, державні стандарти, нормативні документи, постанови, методики та інструкції, які регулюють та контролюють забезпечення інформаційної безпеки країни. До основних задач правової складової належить створення нормативно-правових засад забезпечення інформаційної безпеки, координація діяльності органів державної влади та управління, установ і підприємств із реалізації політики інформаційної безпеки. Аналіз правової складової інформаційної безпеки розуміє аналіз законодавства сфери інформаційної безпеки. На основі аналізу законів України, державних стандартів, нормативно-правових документів системи технічного захисту

інформації визначаються основні проблеми інформаційної безпеки телекомунікаційних систем. Механізм формування вимог до інформаційної безпеки та основні напрями нормативно-правового забезпечення захисту інформації в Україні наведені на рис. 2.2 та 2.3 відповідно.

3. Організаційна складова. Організаційна складова складається з організаційно-правових, організаційно-технічних, організаційно-економічних та організаційно-управлінських аспектів.

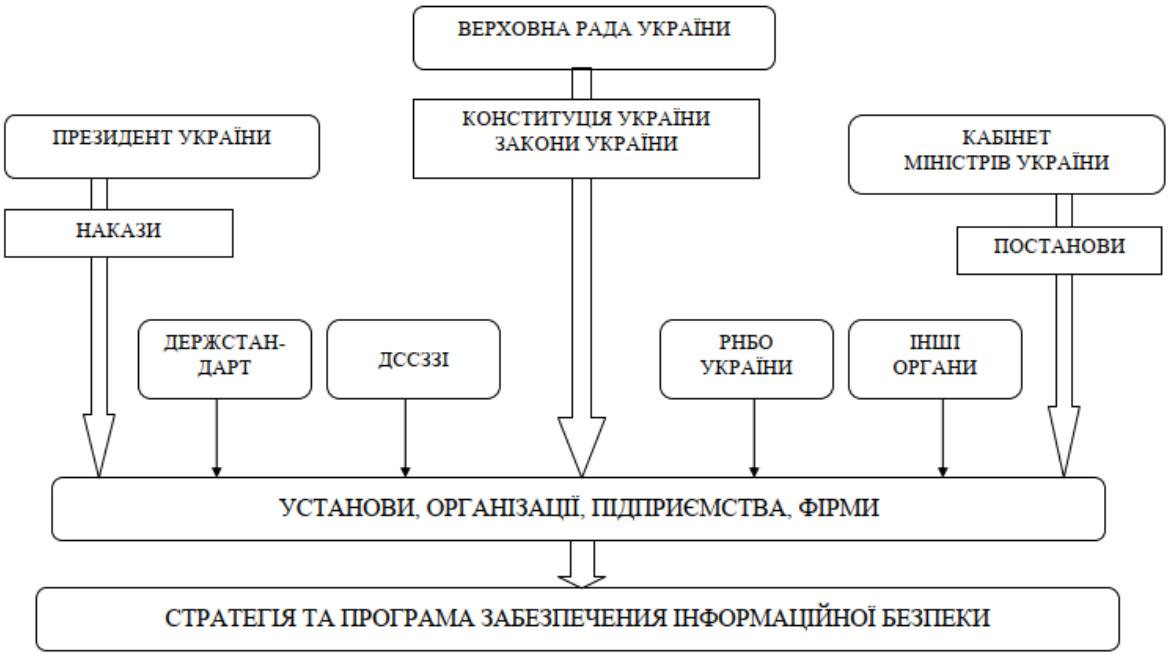

Рис. 2.2 Механізм формування вимог до інформаційної безпеки

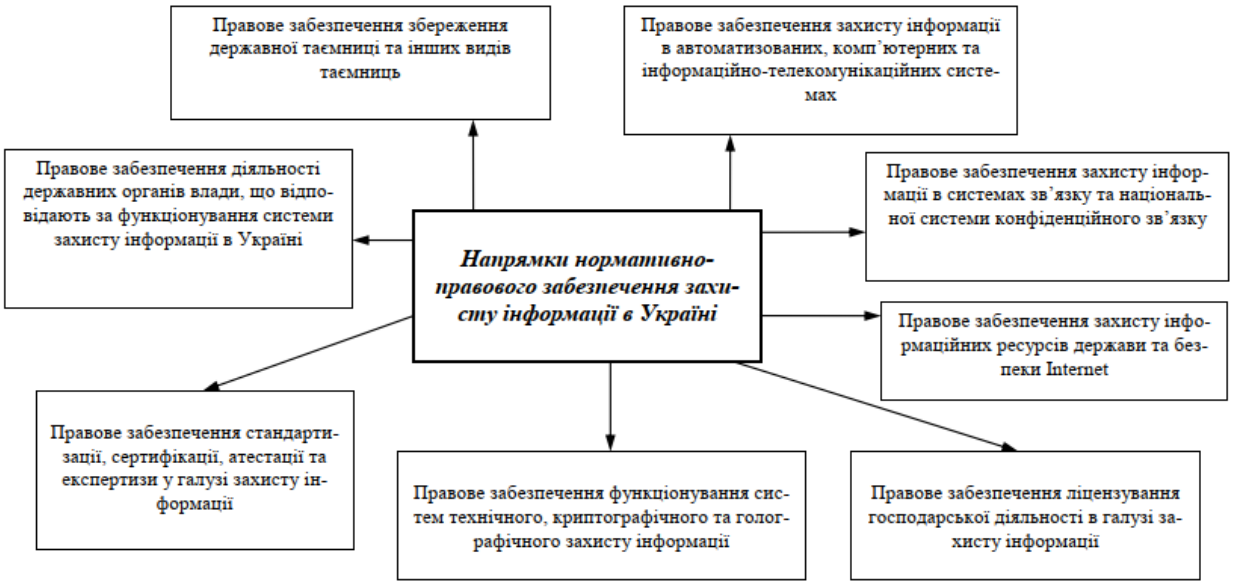

Рис. 2.3 Основні напрями нормативно-правового забезпечення захисту інформації в Україні

Для захисту інтересів суб’єктів інформаційних відносин необхідно поєднувати заходи наступних рівнів: правових (закони, нормативні акти, стандарти і т.п.); управлінських дій загального характеру, організації, що здійснюються керівництвом; та конкретні заходи безпеки, що мають справу з людьми; технічних (конкретні технічні заходи) та економічних заходів.

Організаційно-правовий аспект. Правовий чи законодавчий рівень є найважливішим для забезпечення інформаційної безпеки. Більшість людей не здійснюють протиправних дій не тому, що це технічно неможливо, а тому, що це засуджується і карається суспільством, тому що так поводитись не прийнято.

Розрізняють на законодавчому рівні дві групи заходів: заходи, спрямовані на створення і підтримку в суспільстві негативного (зокрема карального) відношення до порушень і порушників інформаційної безпеки і координуючі заходи, які направляють, сприяють підвищенню утвореної суспільством сфери інформаційної безпеки, що допомагають в розробці і розповсюдженні засобів забезпечення інформаційної безпеки. До першої групи слід віднести, в першу чергу, Закони України «Про інформацію», «Про державну таємницю», «Про телекомунікації» та «Про захист інформації в інформаційно-телекомунікаційних системах» [28-31].

До другої групи відноситься низька документів, що регламентують процеси ліцензування і сертифікації в області інформаційної безпеки. У світі глобальних мереж нормативно-правова база повинна бути узгоджена з міжнародною практикою.

Інформаційна безпека – це нова область діяльності, тут важливо навчити, роз’яснити, допомогти, а не заборонити і покарати. Суспільство повинне усвідомити важливість даної проблематики, зрозуміти основні шляхи розв’язання відповідних задач, повинні бути скоординовані наукові, навчальні і виробничі плани. Держава може зробити це оптимальним чином. Тут не потрібно великих матеріальних витрат, потрібні інтелектуальні вкладення. Приклад позитивного законодавства – Британський стандарт BS

7799:1995, що описує основні положення політики безпеки. Більше 60% крупних організацій використовують цей стандарт у своїй практиці, хоча закон, строго кажучи, цього не вимагає.

Під політикою безпеки розуміється сукупність документованих управлінських рішень, спрямованих на захист інформації та асоційованих з нею ресурсів. Політика безпеки визначає стратегію організації в області інформаційної безпеки, а також ту міру уваги й кількість ресурсів, яку керівництво вважає за доцільне виділити.

Стандарт BS 7799:1995 рекомендує включати в документ, що характеризує політику безпеки організації, такі розділи: ввідний, підтверджує заклопотаність вищого керівництва проблемами інформаційної, безпеки; організаційний, такий, що містить опис підрозділів, комісій, груп тощо, що відповідають за роботу в області інформаційної безпеки; класифікаційні наявні в організації матеріальні та інформаційні ресурси і необхідний рівень їх захисту, що описують штатні, характерні заходи безпеки, вживані до персоналу (опис посад з погляду інформаційної безпеки, організація навчання і перепідготовки персоналу, порядок реагування на порушення режиму безпеки тощо); розділ, що висвітлює питання фізичного захисту; розділ, що описує підхід до управління комп'ютерами і комп'ютерними мережами; розділ, що описує правила розмежування доступу до виробничої інформації; розділ, що характеризує порядок розробки супроводу систем; розділ, що описує заходи, спрямовані на забезпечення безперервної роботи організації; юридичний розділ, що підтверджує відповідність політики безпеки чинному законодавству.

Політика безпеки будується на основі аналізу ризиків, які визнаються реальними для інформаційної системи організації. Коли ризики проаналізовані і стратегія захисту визначена, складається програма, реалізація якої повинна забезпечити інформаційну безпеку. Під цю програму виділяються ресурси, призначаються відповідальні, визначається порядок контролю виконання програми тощо.

Наприклад, заходи захисту від зовнішніх хакерів і від власних скривджених співробітників повинні бути абсолютно різними, тому в першу чергу необхідно визначитися, які загрози здатні нанести найбільшого збитку. Через це зазначимо, що, за статистикою, найбільший збиток відбувається від випадкових помилок персоналу, обумовлених неакуратністю або некомпетентністю, тому в першу чергу важливі не хитрі технічні засоби, а заходи навчання, тренування персоналу і регламентація його діяльності.

Можна виділити наступні групи організаційних заходів, спрямованих на забезпечення інформаційної безпеки: управління персоналом, фізичний захист, підтримка працездатності, реагування на порушення режиму безпеки та планування відновлювальних робіт.

Управління персоналом у контексті інформаційної безпеки, як вже говорилося вище, залишається не проробленим та нерозвиненим питанням. По-перше, для кожної посади повинні існувати кваліфікаційні вимоги щодо інформаційної безпеки. По-друге, в посадові інструкції повинні входити розділи, що стосуються інформаційної безпеки. По-третє, кожного працівника потрібно навчити заходам безпеки теоретично і відтренувати виконання цих заходів практично (проводити подібні тренування двічі на рік.

Охорона організаційно-управлінського аспекту інформаційної безпеки охоплює взаємозв’язані і водночас самостійні напрями діяльності того чи іншого суб’єкта господарювання.

На першій стадії процесу охорони цієї складової інформаційної безпеки здійснюється оцінка загроз негативних дій і можливої шкоди від таких дій. Поміж основних негативних впливів на інформаційну безпеку підприємства виокремлюють недостатню кваліфікацію працівників тих чи тих структурних підрозділів, їхнє небажання або нездатність приносити максимальну користь своїй фірмі. Це може бути зумовлене низьким рівнем управління персоналом, браком коштів на оплату праці окремих категорій персоналу підприємства або нераціональним їх витрачанням. Процес планування та управління персоналом, спрямований на охорону належного рівня інформаційної

безпеки, має охоплювати організацію системи підбору, найму, навчання й мотивації праці необхідних працівників, включаючи матеріальні та моральні стимули, престижність професії, волю до творчості, забезпечення соціальними благами.

Заходи фізичного захисту, відомі з давніх часів, потребують доопрацювання у зв'язку з розповсюдженням мережних технологій і мініатюризацією обчислювальної техніки. Перш за все, слід захиститися від просочування інформації технічними каналами.

Підтримка працездатності – ще одна біла пляма, що утворилася порівняно недавно. В епоху панування великих ЕОМ вдалося створити інфраструктуру; здатну забезпечити, по суті, будь-який наперед заданий рівень працездатності (доступності) на всьому протязі життєвого циклу інформаційної системи. Ця інфраструктура включала як технічні, так і процедурні регулятори (навчання персоналу і користувачів, проведення робіт відповідно до апробованих регламентів тощо). При переході до персональних комп'ютерів і технології клієнт/сервер інфраструктура забезпечення доступності багато в чому виявилася втраченою, проте важливість даної проблеми не тільки не зменшилася, але, навпаки, суттєво зросла.

Реагування на порушення інформаційної безпеки – знову біла пляма. Припустимо, користувач або системний адміністратор зрозумів, що має місце порушення. Що він повинен робити? Спробувати прослідкувати зловмисника? Негайно вимкнути устаткування? Подзвонити в міліцію? Проконсультуватися з фахівцями? Жодне відомство, причетне до інформаційної безпеки, не запропонувало регламенту дій в подібній екстремальній ситуації або свою консультаційну допомогу.

Необхідно організувати національний центр інформаційної безпеки, в коло обов'язків якого входило б, зокрема, відстежування сучасного стану цієї області знань, інформування користувачів усіх рівнів про появу нових загроз і заходи протидії, оперативна допомога організаціям у разі порушення їх інформаційної безпеки. Планування відновних робіт і вся проблематика,

пов’язана з відновленням працездатності після аварій, також потребує уваги. Адже жодна організація від таких порушень не застрахована. Тут необхідно відпрацювати дії персоналу в час і після аварій, заздалегідь потурбуватися про організацію резервних виробничих майданчиків, відпрацювати процедуру перенесення на ці майданчики основних інформаційних ресурсів, а також процедуру повернення до нормального режиму роботи.

Система інформаційної безпеки телекомунікаційних мереж може бути ефективною, якщо витрати на її створення та управління будуть принаймні менші за втрати внаслідок знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення установленого порядку маршрутизації інформації.

Оцінка витрат на захист інформації повинна завжди бути співвідносною з оцінкою втрат, якщо цю інформацію не захищати, та цінністю інформації, а також завжди враховувати можливі ризики. Тоді забезпечення інформаційної безпеки буде насправді якісним.

Завжди оцінюються загрози інформаційній безпеці, що мають політико-правовий характер і включають:

– внутрішні негативні дії;
– зовнішні негативні дії;
– форсмажорні обставини.

Забезпечення інформаційної безпеки компанії має цілком конкретний економічний зміст. А досягнення цієї мети повинне здійснюватися економічно виправданими заходами. Приймати рішення про фінансування проекту з інформаційної безпеки доцільно лише в тому випадку, коли впевнені, що не просто збільшили видаткову частину свого бюджету, а зробили інвестиції в розвиток компанії.

Саме тому організаційно-економічний аспект відіграє не маловажну роль у системі інформаційної безпеки і лежить в основі більшості методів оцінки ефективності вкладень в інформаційну безпеку – зіставлення витрат, необхідних на забезпечення інформаційної безпеки, і збитку, що може бути

заподіяний компанії через відсутність цієї системи. Організаційно-технічний аспект. Згідно з сучасним переконанням, у рамках інформаційних систем повинні бути доступні принаймні такі механізми безпеки: ідентифікація і перевірка справжності (автентифікація) користувачів; управління доступом; протоколювання й аудит; криптографія; міжмережне екранування; забезпечення високої доступності.

Крім того, інформаційною системою в цілому і механізмами безпеки особливо необхідно управляти. І управління, і механізми безпеки повинні функціонувати в різнорідному, розподіленому середовищі, побудованому, як правило, в архітектурі клієнт/сервер. Це означає, що згадані засоби повинні спиратися на загальноприйняті стандарти бути стійкими до мережних загроз, зважати на специфіку окремих сервісів.

На сьогодні переважна більшість розробок орієнтована на платформи Intel/DOS/Windows. В той самий час найбільш значуща інформація концентрується на інших, серверних платформах. Захисту потребують не окремі персональні комп’ютери і локальні мережі на базі таких комп’ютерів, а в першу чергу істотно більш просунуті сучасні корпоративні системи.

Для побудови ешелонованої оборони подібної інформаційної системи необхідні принаймні наступні захисні засоби програмно-технічного рівня: міжмережні екрани (розмежування міжмережного доступу); засоби підтримки приватних віртуальних мереж (реалізація захищених комунікацій між виробничими майданчиками відкритими каналами зв’язку); засоби ідентифікації /автентифікації, що підтримують концепцію єдиного входу в мережу (користувач один раз доводить свою справжність при вході в мережу організації, після чого дістає доступ до всіх наявних сервісів відповідно до своїх повноважень); засоби протоколювання й аудиту, що відстежують активність на всіх рівнях – від окремих застосувань до мережі організації в цілому, що оперативно виявляють підозрілу активність: комплекс засобів централізованого адміністрування інформаційної системи організації; засоби

захисту, які входять до складу застосувань, сервісу й апаратно-програмних платформ.

Практично на усі категорії суб'єктів інформаційних відносин перенесений підхід, розрахований на держструктури.

4. Економічна складова. Економічна складова інформаційної безпеки є невід'ємною, тому що на захист інформації будь-якого підприємства або компанії потрібні гроші, тобто капітальні вкладання. Уся сукупність технічних та організаційних засобів базується саме на економічній складовій, тому цю складову неможливо залишити без уваги чи обійти зовсім.

Економічна складова складається з наступних частин: оцінки витрат на інформаційну безпеку, оцінки втрат від можливих перешкод та зловживань, оцінки можливих ризиків та їх страхування та оцінки цінності інформації.

Система інформаційної безпеки може бути ефективною, якщо витрати на її створення та управління будуть принаймні менші за втрати внаслідок знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення установленого порядку маршрутизації інформації. Неможливо створити абсолютно надійну систему безпеки. Здебільшого через те, що постійно розробляються нові види загроз, яким система не спроможна протистояти, а також через те, що ефективність системи захисту залежить від обслуговуючого персоналу, а людині властиво помилятися.

Вартість подолання захисту повинна бути більше вартості, що досягається при її зломі. У будь-якому випадку вартість засобів забезпечення безпеки повинні відповідати ризику і прибутку в середовищі, який оточує даний суб'єкт.

Керівництво будь-якої компанії розуміє, що неможливо виділити необмежений обсяг фінансів і людських ресурсів на забезпечення інформаційної безпеки. З економічної точки зору вкладення в безпеку повинні показати прибуток або скорочення можливих витрат, що мали місце.

Політика забезпечення інформаційної безпеки повинна визначати пріоритети інвестицій у напряму найбільшої уразливості. Існує низка методів

та методик за допомогою яких оцінюється доцільність витрат на забезпечення інформаційної безпеки підприємства. Але кожне підприємство повинно обирати свій метод чи методику оцінки витрат на інформаційну безпеку, в залежності від специфіки та діяльності підприємства. Але усі існуючі методи об'єднують єдині принципи та правила:

– метод повинен забезпечувати кількісну оцінку витрат на безпеку, використовувати показники оцінки можливостей дій та їх наслідків;

– метод повинен бути прозорим з точки зору користувача та давати можливість уводити особисті емпіричні дані;

– метод повинен бути універсальним, тобто однаково використовуватися до оцінки витрат на закупівлю апаратних засобів, спеціалізованого та універсального програмного забезпечення, витрат на послуги, витрат на переміщення персоналу та навчання користувачів;

– обраний метод повинен дозволяти моделювати ситуацію, за якої існує декілька контрзаходів, спрямованих на попередження виявленої загрози.

На практиці використовуються наступні методи:

– прикладний інформаційний аналіз (Applied Information Economics);

– споживчий індекс (Customer Index);

– доданої економічної вартості (Economic Value Added);

– економічної вартості (Economic Value Sourced);

– управління портфелем активів (Portfolio Management);

– оцінка дійсних можливостей (Real Option Valuation);

– метод життєвого циклу штучних систем (System Life Cycle Analysis);

– система збалансованих показників (Balanced Scorecard);

– сукупної вартості володіння (Total Cost of Ownership);

– функціонально-вартісний аналіз (Activity Based Costing).

5. Соціальна складова. Включає в себе вплив інформації на соціальні процеси та соціально-психологічні аспекти. Відбувається величезне зростання обсягів інформації, знання диференціюються та спеціалізуються, неминуче зростає сфера послуг, тому процес становлення інформаційної цивілізації є об'єктивним і закономірним.

Інформація в сучасному світі вже є засобом і метою повноцінної життєдіяльності та набуває чітких рис реальної влади, яка тісно вплетена в усі сфери функціонування суспільства та всі інші види влади. Людство, таким чином, безупинно просувається до нової ери свого розвитку – ери, де найвищими цінностями виступають інформація та знання.

Як соціальне явище інформатизація охоплює поточні та перспективні проблеми – економічні, організаційні, соціальні, пов'язані з розвитком культури та освіти, діяльністю всіх ланок соціального управління та народного господарства. Як показує досвід інших країн, інформатизація сприяє забезпеченню національних інтересів, розвитку наукомістких виробництв та високих технологій, підвищенню продуктивності праці, удосконаленню управління економікою, соціально-економічних відносин, збагаченню духовного життя та подальшої демократизації суспільства.

Тому соціальна складова є також невід'ємною для забезпечення інформаційної безпеки. З визначення складових ІБ підприємства випливає, що для того, щоб перейти до методів та засобів захисту конфіденційної інформації на підприємстві необхідно розглянути джерела загроз інформації.

2.2 Інтегрована система управління якістю навчального закладу

Із 2015 р. упроваджена система управління якістю, сертифікована на відповідність вимогам стандарту ISO 9001:2008.

У квітні 2019 р. за результатами планового аудиту аудиторська група рекомендувала органу DQS підтвердити сертифікат відповідності системи управління якістю НФаУ вимогам стандарту ISO 9001:2015.

01 березня 2021 р. НФаУ отримав сертифікати Міжнародної організації із сертифікації (ISO) на відповідність вимогам стандартів ISO 14001:2015 та

ISO 50001:2018, які підтверджують дію в університеті екологічного та енергетичного менеджменту.

На теперішній час в університеті одночасно діє три стандарти ISO (системи управління якістю, еко- та енергоменеджменту), а сама система набула статусу Інтегрована система управління (ІСУ НФаУ).

Місія НФаУ – розвиток національної галузі охорони здоров'я за рахунок здійснення всебічної підготовки компетентних фахівців на рівні стандартів Європейського простору вищої освіти.

Бачення: Ми – загальновизнаний заклад вищої освіти фармацевтичного та медичного спрямування, лідер національних рейтингів та гідний представник української наукової школи в європейських і світових рейтингах навчальних закладів.

Для реалізації місії колектив університету постійно і наполегливо працює над:

– підвищенням компетентності науково-педагогічних працівників;

– удосконаленням методів і засобів ведення освітнього процесу, підвищенням результативності виховної та профорієнтаційної роботи;

– удосконаленням навчально-методичної та матеріально-технічної бази;

– неухильним виконанням законодавчих вимог та добровільно взятих на себе зобов'язань;

– розширенням і укріпленням міжнародних зв'язків;

– підвищенням рівня наукових досліджень та участь у формуванні визнаних в Україні та у світі наукових шкіл;

– зменшенням екологічних впливів та запобіганням забрудненню навколишнього середовища;

– удосконаленням робіт з ефективної експлуатації енергетичного обладнання, закупівлі енергоефективної продукції та послуг, розробки й реалізації енергоефективних проєктів.

Досягнення поставлених цілей значною мірою планується здійснювати завдяки результативному функціонуванню системи управління якістю, що побудована відповідно до вимог Інтегрованої системи управління [32].

Інформація може бути загальнодоступною, та закритою, вона може бути захищеною, та, у той же час, відкритою для загалу, змінною або недостовірною, тощо. Кожна компанія, від маленького підприємства до великих корпорацій має власне ставлення до інформації. Всі хочуть отримати якомога більше інформації стосовно ринків збуту продукції, виробництва, фінансової інформації, даних про конкурентів та партнерів, у той же час зберегти в таємниці свою комерційну інформацію, втрата, або розповсюдження якої може фатально вплинути на діяльність компанії та її позицій на ринку. Основні ризики, які можуть бути розглянуті щодо інформації підприємства, пов’язані з неправильним підходом до керування інцидентами інформаційної безпеки; незахищеністю активів IT-інфраструктури; неналежним захистом інформації у мережах та на носіях з використанням технічних уразливостей цих самих носіїв, тощо.

Дерево процесів ЗВО містить забезпечуючий процес: А3.4 – Забезпечення ІТ інфраструктури та підпроцес: А3.4.1 – Забезпечення належного технічного стану ІТ інфраструктури, який націлений на :

1. Запровадити пропускну систему до корпусів та гуртожитків за електронними перепустками 2021 р.

2. Створити програму розвитку ІТ-структури НФаУ 2021 р.

3. Розробити та здійснити план розвитку автоматизованої системи управління "Університет" 2021 р.

4. Розробити концепцію інформатизації та комп’ютеризації університету, комплекс заходів з її реалізації 2020 р.

5. Розробити та запровадити систему забезпечення безпеки інформаційного середовища і збереження корпоративних даних 2020 р.

6. Створити групу адміністрування серверної інфраструктури та комп’ютерних мереж НФаУ, групу інформаційного супроводу адміністративно-фінансових систем НФаУ 2021 р.

7. Забезпечити технічну підтримку впровадження системи електронного документообігу 2025 р.

Також містить підпроцес: А3.4.2 – Технічне забезпечення дистанційного навчання, який повинен:

1. Створити відкритий масовий on-line курс «Вступ у фармацію» на платформі Prometeus 2020 р.

2. Запровадити програму підвищення компетентності науково-педагогічних працівників з питань використання дистанційних технологій у навчальному процесі 2025 р.

3. Закінчити розробку та провести сертифікацію дистанційних курсів за спеціальністю "226 Фармація, промислова фармація" 2020 р.

4. Створити дві нових on-line студії 2020 р.

5. Розробити та впровадити у навчальний процес лабораторні стемулятори 2025 р [33].

В сучасному бізнес-середовищі ефективна комунікація та інноваційний менеджмент є важливими компонентами. Комунікація є ключовим елементом для досягнення мети організації, сприяє обміну інформацією, координації дій та підвищенню рівня співпраці всередині та поза організацією. Тому робота з інформаційними потоками та захист інформації є одними з ключових завдань системи управління ЗВО.

Висновки до розділу 2

В 2 розділі автором описано складові інформаційної безпеки підприємства, які включають організаційно-управлінські, правові, економічні, соціальні та технічні особливості роботи з інформацією організації зовнішнього та внутрішнього характеру.

Також автор дослідив роботу інтегрованої системи управління ЗВО та відповідну процесну модель, яка містить забезпечувальний процес, що має відповідні завдання щодо побудови інформаційного захисту університету.

РОЗДІЛ 3

ПРАКТИЧНІ ПІДХОДИ ДО ФОРМУВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОГО ЗАХИСТУ УНІВЕРСИТЕТУ

3.1 Організація кроків впровадження системи інформаційного управління університету

В умовах гібридних загроз інформаційна безпека представляє набір інструментів та методів для захисту різних видів інформації та реагування на виникнення нових загроз у стані невизначеності. Вона включає безліч сучасних інформаційних технологій, використання яких стає необхідністю успішного функціонування підприємства.

Під інформаційною безпекою розуміється стан інформаційного середовища, який забезпечує розвиток цього середовища, ефективне використання інформації в інтересах підприємства, а також захищеність від будь-яких загроз та спроможність реагувати та змінюватись в залежності від внутрішніх і зовнішніх факторів, задля забезпечення безпечної діяльності підприємства. Забезпечення інформаційної безпеки на підприємстві слід розглядати як невід'ємний елемент процесу управління підприємством, в контексті існування гібридних загроз, невдале керування підприємством ставить під сумнів безпекові характеристики підприємства [34, 35].

Стандарт є робочим інструментом для впровадження СУІБ в організації, а також для проведення аудиту з підтвердження того, що засоби управління безпеки функціонують відповідно до вимог стандарту. Стандарт описує СУІБ як всеохоплюючу систему менеджменту, побудовану на принципах бізнес-ризиків, для впровадження, експлуатації, моніторингу та підтримки системи менеджменту безпеки [36].

Відповідно до ISO 27001, система управління інформаційною безпекою – це «та частина загальної системи управління організації, заснованої на оцінці бізнесризиків, яка створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід і вдосконалення інформаційної безпеки».

Система управління містить структуру організації, політики, планування, посадові обов’язки, практики, процедури, процеси і ресурси. Створення та експлуатація СУІБ вимагає застосування такого ж підходу, як і будь-яка інша система управління. Варто окремо вказати на стратегічні переваги, які може отримати бізнес від сертифікації згідно із стандартом ISO 27001 [37]:

– побудова надійної структури інформаційної безпеки; – захист даних та інтелектуальної власності;

– створення нових можливостей (наприклад, співпраця з фінансовими компаніями);

– підвищення лояльності клієнтів;

– уникнення фінансових і репутаційних втрат, пов’язаних з дискредитацією даних;

– зростання довіри інвесторів;

– запобігання кібератакам і витоку даних;

– отримання конкурентної переваги на ринку.

Використовувана в ISO 27001 для опису СУІБ процесна модель передбачає безперервний цикл заходів PDCA (Plan-Do-Check-Act): планування, виконання, перевірка, вплив (управління, коригування) [38], відомий як цикл Шухарта-Демінга (рис. 3.1, табл. 3.1).

Застосування СУІБ є однією з умов активного розвитку бізнесу, її використання при виникненні гібридних загроз інформаційним системам підприємства забезпечує спроможність до попереднього виявлення, протистояння загрозі та подальшого існування. Використання методів ризик-менеджменту, а також застосування інших технічних та організаційних процедур, методів, програмного та технічного забезпечення, зумовлює досягнення реалізації інформаційної безпеки підприємства спроможної протистояти гібридним загрозам.

Реалізація системи управління інформаційною безпекою може бути організовано як дерево процесів. Створення ефективної системи управління

інформаційною безпекою можна описати певною послідовністю заходів на підприємстві, така послідовність може включати етапи, які наведені на рисунку 3.2.

Рис. 3.1 Модель PDCA для впровадження СУІБ

Таблиця 3.1

Опис циклу PDCA для впровадження СУІБ

PDCA	Опис
Планування	Розроблення політики безпеки, визначення мети, процесів та процедур, пов’язаних з управлінням ризиками та підвищенням інформаційної безпеки для досягнення результатів відповідно до загальної політики та цілей організації
Виконання	Впровадження та використання політики безпеки, елементів керування, процесів та процедур, механізмів контролю
Перевірка	Оцінювання та вимірювання ефективності роботи відповідно до політики безпеки, цілей та практичного досвіду, а також підготовка звіту про результати для керівництва з метою подальшого аналізу й аудиту
Вплив (управління, коригування)	Застосування коригувальних та профілактичних заходів з метою досягнення постійного вдосконалення СУІБ на основі результатів аналізу; перегляд політики безпеки; підвищення поінформованості персоналу

Фактична реалізація етапів формування системи управління інформаційною безпекою залежить від специфіки конкретного підприємства. Етапи формування визначають впровадження відповідних заходів, виконання дій або прийняття рішень, які можна поділити на три блоки.

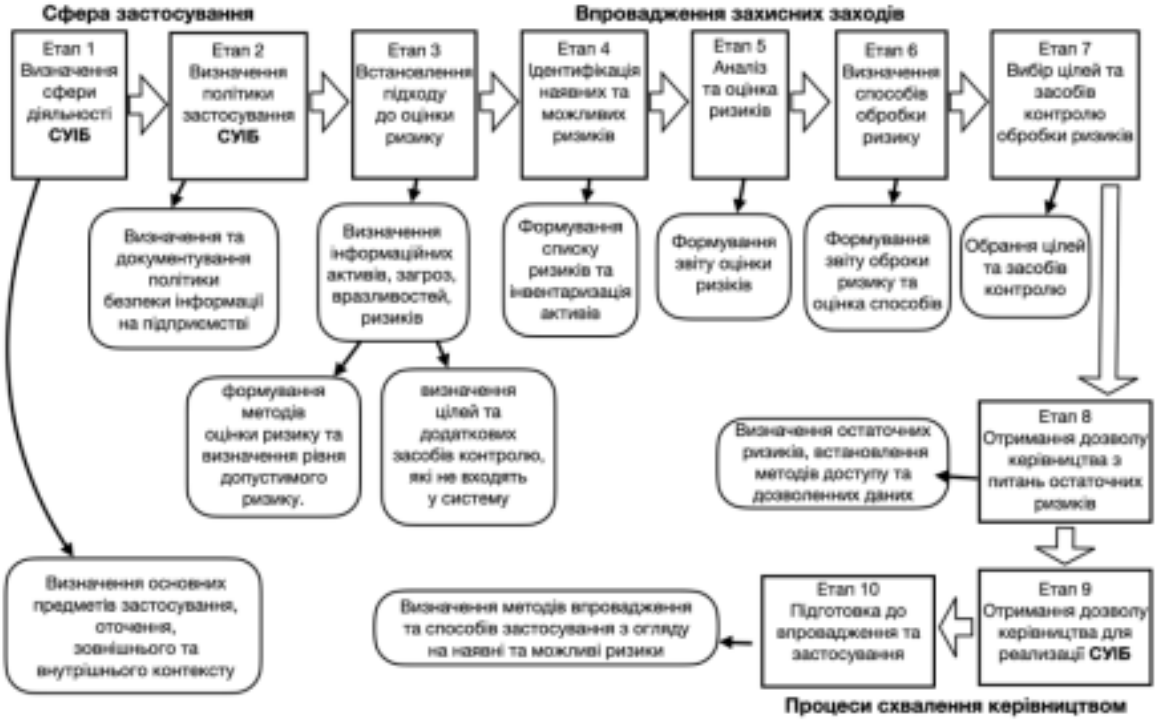

Рис. 3.2 Послідовність формування системи управління інформаційною безпекою на підприємстві

Перший та другий етап забезпечують встановлення сфери застосування СУІБ.

З третього по сьомий етапи відбувається впровадження захисних заходів на основі ризик-менеджменту.

Етапи 8-10 зазначають процеси схвалення керівництвом рішень для впровадження засобів обробки ризиків, формулювання вимог, та дозволів на реалізацію та використання механізмів системи.

Враховуючи велику кількість процесів інформаційної безпеки під час діяльності підприємства, ефективна СУІБ повинна враховувати засоби призначені для розробки, впровадження, функціонування, моніторингу, перегляду, підтримування, а також розвитку та вдосконалення інформаційної безпеки.

Також важливо враховувати вже напрацьовані стандарти, які допоможуть реалізувати ефективну у використанні систему, такі стандарти, пропонують сформовані вимоги до побудови, методи використання та засоби розвитку СУІБ на підприємстві.

Розглянемо процес впровадження більш детально:

Етап 1. Затвердження рішення про створення СУІБ. Рішення про створення СУІБ повинно прийматися керівниками компанії. Відділ захисту інформації (служба інформаційної безпеки) реалізовує початок даного процесу. У разі вирішення прийняття системи менеджменту інформаційної безпеки керівництво повинно усвідомлювати кінцеву ціль даного заходу та важливість сертифікації для бізнесу.

Етап 2. Попередня підготовка. Наступним етапом є створення робочої групи та призначення керівника. До її складу мають увійти: представники керівництва університету, представники відділів, старші спеціалісти, що забезпечують інформаційну безпеку. Дані співробітники повинні усвідомленні про механізми систем менеджменту. До складу робочої групи можуть входити також консультанти, що спеціалізуються на питаннях СУІБ. Робоча група повинна мати всю необхідну нормативно-методичну базу для успішного створення, відповідно вимогам.

Попередній аналіз оцінює галузі діяльності організації, які будуть охоплені СУІБ. При виборі області діяльності, в якій робоча група буде впроваджувати механізми СУІБ, повинні враховуватися наступні критерії: діяльність та послуги, що надаються організацією своїм партнерам і клієнтам, цільова інформація, безпека якої повинна бути забезпечена, бізнес-процеси, що забезпечують обробку інформації, відділи і співробітники організації, задіяні в даних бізнес-процесах, програмно-технічні засоби, що забезпечують функціонування даних процесів, територія компанії, в рамках яких відбуваються збір, обробка та передача інформації.

Результатом є узгоджена та затверджена з керівництвом область діяльності університету, в рамках якої планується створення СУІБ. Також в

процесі створення системи потрібно постійно аналізувати та виявляти невідповідності до нормативних документів. Для уточнення обсягу робіт і необхідних витрат на створення і подальшу сертифікацію СУІБ, члени робочої групи проводять роботи з виявлення й аналізу невідповідностей існуючих в організації заходів захисту до вимог стандарту. При цьому аналізуються як прийнятті організаційні заходи по плануванню, впровадженню, аудиту та модернізації, так і використовувані програмно-технічні засоби і механізми захисту інформації. На даному етапі університет також може вибрати незалежний орган з сертифікації систем менеджменту, що має відповідну акредитацію.

Етап 3. Аналіз ризиків. Найбільш складним завданням, що вирішуються в процесі створення СУІБ, слід назвати проведення аналізу ризиків інформаційної безпеки щодо активів в обраній галузі діяльності та прийняття керівництвом рішення про вибір заходів для зменшення ризиків У процесі аналізу ризиків проводяться наступні роботи: ідентифікація всіх активів в рамках обраної діяльності, визначення цінності активів, ідентифікація загроз і вразливостей для даних активів, оцінка ризиків для можливих випадків успішної реалізації загроз, вибір критеріїв прийняття ризиків, підготовка плану оброблення ризиків. Виконання всіх зазначених завдань зазвичай здійснюється відповідно до розроблюваної процедури аналізу ризиків, в якій визначена методологія і відображені організаційні аспекти.

Важливою ланкою аналізу ризиків є ідентифікація та визначення цінності активів. У рамках даних робіт повинні бути розглянуті всі бізнес-процеси, що входять в обрану область діяльності організації. По кожному бізнес-процесу, проводиться ідентифікація активів, а саме: інформаційні вхідні дані, вихідні дані, оброблювальні данні, працівники обраної галузі, інфраструктура, обладнання, програмне забезпечення. Наступним кроком у проведенні аналізу ризиків, щодо активів університету є визначення цінності активу, яка виражається у величині збитку для організації.

Інформація про цінності активу може бути отримана від його власника або ж від особи, якій власник надав всі повноваження з даного активу. Результатом даних робіт є звіт про ідентифікацію та оцінку цінності активів. Власне аналіз ризиків – це основний періодичний процес СУІБ. Необхідно підібрати таку методику аналізу ризиків, яку можна було б використати з мінімальними затратами часу та ресурсів.

Можна використовувати існуючу чи розробити власну методику, яка найкращим чином підходитиме до специфіки діяльності. У процесі аналізу ризиків для кожного з активів або групи активів проводиться ідентифікація можливих загроз і вразливостей, оцінюється ймовірність реалізації кожної загрози і, з урахуванням величини можливого збитку для активу, визначається величина ризику, що відображає критичність загрози. В процедурі аналізу ризиків повинні бути ідентифіковані критерії прийняття ризиків та допустимі рівні ризику.

Ці критерії мають базуватися на стратегічних, організаційних та управлінських цілях організації. Керівники компанії використовують дані критерії, приймаючи рішення щодо прийняття контрзаходів для протидії виявленим ризикам. Якщо виявлений ризик не перевищує встановленого рівня, він є прийнятним, і подальші заходи по його обробці не проводяться. У випадку, якщо виявлений ризик перевищує прийнятний рівень, повинне бути прийняте одне з рішень: зниження ризику до прийнятного рівня за допомогою застосування відповідних контрзаходів; прийняття ризику; уникнення ризику; передача ризику.

Після ідентифікації та опису можливих ризиків слідує під етап – «План обробки ризиків». Створюваний на даному етапі документ містить перелік першочергових заходів щодо зниження рівнів ризиків, а також цілі та засоби управління, спрямовані на зниження ризиків, із зазначенням: осіб, відповідальних за реалізацію даних заходів, термінів реалізації та пріоритетів їх виконання, ресурсів, рівнів залишкових ризиків. Прийняття плану обробки ризиків та контроль за його виконанням здійснює керівництво організації.

Виконання ключових заходів плану є відправною точкою для прийняття рішення про введення СУІБ в експлуатацію.

Етап 4. Розробка політик і процедур СУІБ. Розробка організаційно-нормативної бази, необхідної для функціонування СУІБ, може проводитися паралельно з реалізацією заходів плану обробки ризиків. На даному етапі розробляються документи СУІБ. Зазвичай сюди входять такі політики та процедури: область діяльності, політика СУІБ. Також відносяться механізми забезпечення ІБ, такі як: політика антивірусного захисту; політика надання доступу до інформаційних ресурсів; політика використання засобів криптографічного захисту, тощо.

Процедури ж можуть містити такі наступні заходи: управління документацією, управління записами, внутрішні аудити, коригувальні дії, попереджуючі дії, управління інцидентами, аналіз функціонування СУІБ керівництвом організації, оцінка ефективності механізмів управління СУІБ, інші процедури та інструкції. Розроблені політики та процедури повинні охоплювати наступні ключові процеси СУІБ: управління ризиками, управління інцидентами, управління ефективністю системи, управління персоналом, управління документацією та записами системи управління ІБ, перегляд і модернізація системи, управління безперервністю бізнесу і відновлення після переривань. Крім того, в посадові інструкції відповідального персоналу, положення про підрозділи, контрактні зобов’язання організації повинні бути включені обов’язки щодо забезпечення інформаційної безпеки.

Обов’язки з виконання вимог СУІБ за допомогою відповідних наказів та розпоряджень покладаються на відповідальних співробітників відділів. Всі розроблені положення політики, процедури та інструкцій доводяться до відома рядових співробітників при їх навчанні та інформуванні. Таким чином, в результаті не тільки створюється документальна база СУІБ, але й відбувається реальний розподіл обов’язків щодо забезпечення безпеки інформації серед персоналу.

Етап 5. Впровадження СУІБ в експлуатацію. Датою введення СУІБ в експлуатацію є дата затвердження компанії положення про внутрішній регламент обробки інформації. Даний документ є публічним і декларує цілі та засоби, обрані організацією для управління ризиками. Положення включає наступне: засоби управління і контролю, вибрані на етапі обробки ризиків, існуючі в організації засоби управління, засоби, що забезпечують виконання вимог законодавства, засоби, що забезпечують виконання загально корпоративних вимог, тощо. При введенні СУІБ в експлуатацію використовуються всі розроблені механізми, що реалізують обрані цілі.

Таким чином системи управління інформаційною безпекою є невід'ємною частиною загального управління підприємством, вони забезпечують стійкість інформаційних структур до внутрішніх та зовнішніх загроз а також дозволяють впроваджувати заходи щодо розвитку, завдяки можливості прогнозувати стан підприємства відносно можливих загроз.

Великий досвід застосування міжнародних стандартів формування систем управління інформаційною безпекою, який базується на основі менеджменту ризиків, дозволяє будувати системи, які спроможні захищати підприємство та забезпечувати його розвиток.

Треба також зазначити, що під час реалізації інформаційної безпеки перед університетом постає задача у пошуку ефективного балансу між відповідністю системи та її засобів конкретному виду діяльності, зручністю використання та рівнем забезпечення безпеки інформації.

3.2 Розробка політики та цілей системи інформаційної безпеки

Розширення IT-інфраструктури та інформаційних технологій тягне з собою появу все більшої кількості ризиків і сфері інформаційної безпеки. Надійний партнер має усвідомлювати і задекларувати шляхом добровільної сертифікації рівень відповідальності за збереження конфіденційності не лише власних даних, а також і сторонніх інформаційних ресурсів.

Політика інформаційної безпеки – це сукупність правил і принципів, якими керується компанія в цій області, в тому числі і з метою виконання умов сертифікації.

Оскільки організація інформаційної безпеки має здійснюватися шляхом комплексного підходу, політика інформаційної безпеки має встановлювати відповідальність вищого керівництва, його цілі і принципи щодо дотримання інформаційної безпеки.

Крім того, політика містить загальне визначення інформаційної безпеки як можливості спільного використання інформації, законодавчий і правовий аспект питання, навчання персоналу з питань цієї сфери, протидії появі шкідливого програмного забезпечення, обов'язки персоналу, відповідальність за порушення власне політики безпеки, а також управління безперервністю бізнесу.

Розробка політики інформаційної безпеки є початковим етапом процедури проведення сертифікації та починається з аналізу ризиків у цій сфері, в тому числі і визначення оптимального рівня ризику. Досягнення такого рівня має стати визначальною віхою та метою розробки системи управління інформаційною безпекою.

Наступний етап розробки – аналіз інформаційних ресурсів, визначення їх цінності та побудова моделі взаємозв'язків між ними. Отримана модель дає можливість обрати оптимальні способи протидії інформаційних ризикам та дотримуватися загальної схеми сертифікації системи управління.

Останній крок – розробка документації у сфері забезпечення інформаційної безпеки.

Результатом цих дій має бути створення документа, що вбирає в себе основні принципи і правила, яких дотримується компанія для забезпечення інформаційної безпеки – власне політики інформаційної безпеки.

Нами було запропоновано Політику інформаційної безпеки для університету, де ми зазначаємо, що для досягнення основної мети, ми використовуємо такі принципи (Додаток А та Додаток Б):

– Надання освітніх послуг з можливістю онлайн навчання за графіком та на основі оптимальних інформаційних умов.

– Досягнення задоволення зацікавлених сторін якістю наданих освітніх послуг.

– Забезпечення високого рівня професійної підготовки персоналу та підвищення ІТ-обізнаності.

– Оснащення сучасним, професійним обладнанням та застосування передових технологій для ефективного здійснення освітніх послуг.

– Підвищення рівня безпеки персональних та корпоративних даних.

– Оптимізація використання кадрових-, матеріальних- та фінансових- ресурсів для рішення завдань у сфері забезпечення безпеки інформації.

– Ректор університету несе відповідальність за розробку, впровадження та функціонування системи забезпечення інформаційної безпеки відповідно до вимог міжнародних стандартів та постійне підвищення її результативності.

– Ця Політика є основою для роботи персоналу всіх структурних підрозділів/кафедр, реалізується системою забезпечення інформаційної безпеки і знаходиться під особистим контролем Ректора університету.

– Керівництво бере на себе відповідальність за реалізацію Політики у сфері безпеки інформації і зобов'язується забезпечити її розуміння та виконання всіма співробітниками університету.

3.3. Етапи ідентифікації інформаційних активів

Об’єктом СУІБ є інформаційні активи, тобто матеріальні або нематеріальні об’єкти, які є інформацією, або містять інформацію, або необхідні для оброблення інформації. Інформаційні активи володіють основними властивостями фінансових і матеріальних активів підприємства. Загалом цінність інформаційних активів набагато більша за фінансові активи

університету, оскільки більшість діяльності пов'язана з інтелектуальною власністю.

Межі СУІБ включають організаційні одиниці, бізнес-підрозділи, інформаційні системи та інші складові підприємства. Таким чином, інвентаризація активів проводилась за всіма бізнес-одиницями університету. Процес інвентаризації включив у себе:

– ідентифікацію бізнес-процесів;
– ідентифікацію інформаційних активів;
– ідентифікація власників активів;
– ідентифікацію фізичних та інформаційних ресурсів;
– визначення місць зберігання інформаційних активів.

Всі бізнес-процеси визначались через відповідні структурні відділи університету, в рамках яких вони циркулюють. Розглядаються такі структурні підрозділи (рис. 3.3.):

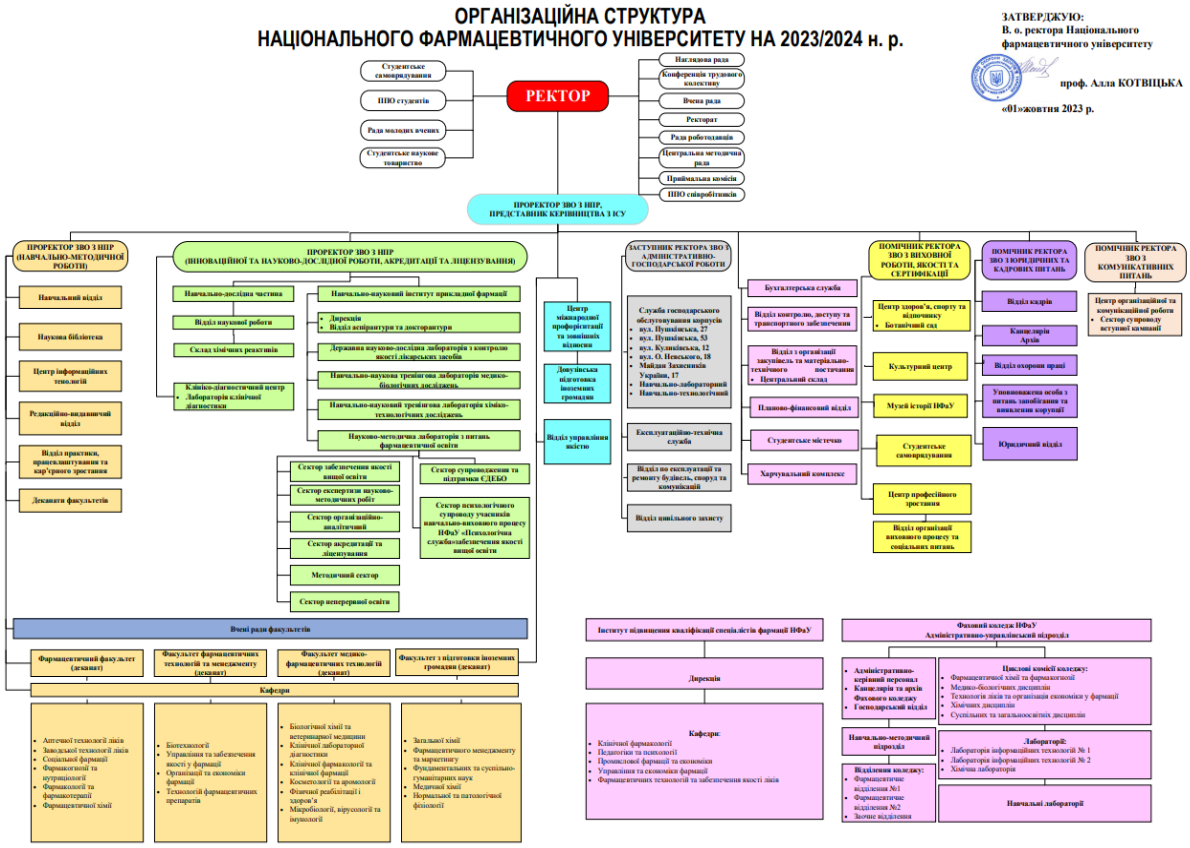

Рис. 3.3 Організаційна структура НФаУ

Після ідентифікації всіх бізнес-процесів, було визначено всіх власників інформаційних активів. Як правило, це керівники бізнес-напрямків.

Такі керівники мають повноваження і відповідальність для захисту важливої для бізнесу інформації. Власники бізнес-процесів є також власниками інформаційних активів, які створюються та / або використовуються в рамках їх напрямків діяльності.

Власники бізнес-процесів повинні мати необхідні знання, щоб визначити критичність активу, і повинні мати повноваження, щоб організувати захист активу від порушення конфіденційності, цілісності та доступності. Обов'язки власника можуть бути делеговані, однак відповідальність повинна залишатися за призначеним власником активу.

Тому нами розроблено матрицю відповідальності (табл. 3.2):

Таблиця 3.2.

Матриця відповільності щодо кроків впровадження СУІБ

	Ректор	**Перший проректор**	**Бухгалтер**	**Керівник відділу кадрів**	**Керівники інших відділів**
	Управлінські процеси				
Розробка та затвердження цілей в сфері інформаційної безпеки	Відп	Вик	Вик	Вик	Вик
Планування роботи	Відп	Вик	Вик	Вик	Вик
Розробка стратегічних планів та програм	Відп	Вик	Вик	Вик	Вик
Аналіз зовнішніх ресурсів	Відп	Вик	Вик	Вик	Вик
Аналіз внутрішніх потреб	Контр	Відп	Вик	Вик	Вик
SWOT-аналіз	Контр	Відп	Вик	Вик	Вик
Визначення порядку виконання взаємодії бухгалтерії	Контр	Відп	Вик	Вик	Вик

Визначення порядку виконання взаємодії структурних підрозділів	Контр	Відп	Вик	Вик	Вик

Вик. – виконавець; Контр. – контролер; Відп. – відповідальний.

Згідно визначеної підприємством методики, було створено реєстр активів, тобто сформована таблиця в якій перераховані існуючі активи організації . Опис активів відбувався за допомогою таких параметрів:

– назва активу;
– рівні забезпечення;
– носії інформаційного активу;
– власник активу;
– місце знаходження активу;
– категорія активу.

В таблиці виділено три рівні забезпечення: конфіденційність, цілісність, доступність.

Власником активу призначено особу, яка реально працює з активом і здатна впливати на властивості і стан активу. Інформаційний актив – це будь яка інформація (відомість), яка представляє цінність для підприємства, його клієнтів, ділових партнерів та співробітників, а також будь-яка система для обробки інформації або фізичного місця її зберігання. Для ідентифікації інформаційних активів проводилося інтерв'ю з кожним із визначених власників бізнес-процесів. В результаті опитування було визначено:

– яка інформація створюється і обробляється підрозділами в електронному та паперовому вигляді;
– фізичні місця, де інформація зберігається і обробляється, включаючи автоматизовані системи, файлові сервера, локальні комп'ютери, паперові документи, зовнішні місця зберігання (наприклад, системи контрагентів або постачальників) і фізичні локації;
– кожного користувача, який має доступ і працює з інформацією в або поза підприємством, із зазначенням посади, підрозділу (відділу);

– критичність інформації для підприємства;

– визначено рівні наслідків при порушені конфіденційності, цілісності та доступності (табл. 3.3)

Таблиця 3.3.

Наслідки при порушенні КЦД

Рівень наслідків порушення КЦД	Опис наслідків порушення
4	Критичні наслідки, не зворотні (втрата частини ринку, закриття проектів, критичне зниження лояльності співробітників)
3	Дуже важливі наслідки, не зворотні (значні матеріальні втрати, отримання матеріальної вигоди конкурентами, Погіршення клімату в колективі)
2	Важливі наслідки, але зворотні (порушення приведуть до неправильної роботи інформаційних активів)
1	Значні наслідки, результати від яких проявляться через деякий час, без порушень в роботі
0	Незначні порушення (наслідки відсутні)

3.4. Розробка програми впровадження СУІБ в діяльність університету

Програма впровадження системи управління інформаційної безпеки є інструментом управління, який повинен інтегруватися в СУІБ університету на базі принципів стандарту ISO 27001.

Програма складається з чотирьох етапів. Для кожного встановлено часові рамки виконання роботи. На основі цього прописано ймовірні результати, які мають бути отримані за результатами виконання програми з реалізації принципів СУІБ.

В перелік робіт було включено:

– оцінка загроз діяльності;

– аналіз наявної документації та розробка тієї, що не вистачає для нормального виконання робіт з СУІБ;

– проведення аудиту та аналіз його результатів;

– навчання персоналу на основі програми.

Стратегічне планування проводиться на першому етапі, на який ми виділили 85 робочих днів. Він включає:

– затвердження наказу;

– формування робочої групи з персоналу.

Термін виконання - 10 робочих днів. Відповідальний за виконання першого етапу – ректор. В завершення першого етапу видається наказ про початок роботи для створення СУІБ. В ньому зазначається перелік учасників робочої групи із зазначенням їх обов'язків та повноважень.

Другий етап включає проведення аудиту щодо загроз для ведення нормальної стабільної діяльності та визначення критичних процесів виконання послуг щодо СУІБ на підприємстві. За результатами етапу складається звіт. В ньому викладено оцінку ризиків потенційних ІТ-загроз. Термін виконання - 20 робочих днів.

Термін виконання діагностики ресурсів підприємства - 5 днів. Обов'язок контролювати належне виконання процесу покладається на головного аудитора. За результатами етапу складається звіт для його подальшої оцінки вищим керівництвом.

Головний бухгалтер розраховує економічну можливість здійснення СУІБ. На основі цього надається фінансовий звіт щодо економічних ресурсів самого підприємства.

Вищим керівництвом розробляється політика та цілі в сфері СУІБ. Термін виконання етапу – 15 робочих днів.

Керівник відділу кадрів відповідальний за проведення навчання персоналу. Весь процес фіксується в протоколах навчання. В кінці етапу призначаються відповідальні особи з розподілом між ними основних обов'язків.

На другому етапі розробляється план впровадження СУІБ. Термін його реалізації - 70 робочих днів.

На початку визначається перелік критичних процесів та виділення конкретних ресурсів на зменшення кількості ризиків. Ректор є відповідальною особою. Підсумком виконання даного етапу є специфікація критичних процесів та розподіл наявних ресурсів для їх виконання в умовах надзвичайних ситуацій.

Начальники підрозділів та завідувачі кафедр надають список співробітників, які будуть брати участь у функціонуванні СУІБ із зазначенням їх обов'язків. На основі цього відповідним розпорядженням ректора затверджується матриця відповідальності. Після цього голова відділу кадрів вносить зміни до посадових інструкцій.

На основі інформації, отриманої під час виконання обох етапів складається та затверджується план. До нього додаються затверджені протоколи СУІБ.

2 етап завершується інформуванням та навчанням співробітників підприємства щодо Політики та цілей в сфері СУІБ.

На 3 етапі створюється система документообігу. Термін реалізації - 50 робочих днів.

Аналізується структура існуючої документації та впровадження нової розробленої документації щодо СУІБ. На основі цього формується загальний перелік документів. Далі розробляються документовані процедури та інструкції для належного виконання дій в аварійних ситуаціях. В їх основу лягає процедура управління документами. Співробітників ознайомлюють з новою документацією. Цей процес контролюється головами підрозділів.

На основі результатів аналізу наявної документації складається та затверджується План-графік розробки нових документів. Термін виконання - 5 робочих днів з можливістю подовження під час формування СУІБ.

Щодо впровадження нової документації та правил її оформлення проводиться інформування та навчання персоналу. Розроблені документи розповсюджуються та адаптуються до діяльності на основі наказу ректора.

Термін проведення навчання - 10 днів. За навчання працівників відповідають начальники підрозділів, які проводять заняття згідно з програмою. Задля подальшого аналізу керівництвом результати навчання фіксуються у протоколах.

На 4 етапі СУІБ впроваджується в діяльність університету. Термін виконання - 45 робочих днів.

Перший крок - розповсюдження у підрозділах розробленої документації СУІБ з картками обліку та листами ознайомлення.

Навчання персоналу щодо реалізації програми СУІБ проходитиме за встановленим планом. Воно буде здійснюватися постійно. Результати фіксуватимуться записами в протоколах навчання та оцінкою результатів керівництвом.

Наступною буде організація та проведення внутрішніх аудитів на відповідність вимогам ISO 27001. Відповідальний за цей процес - головний аудитор.

На завершення робіт з формування програми СУІБ ректор може прийняти рішення щодо оформлення заявки на сертифікацію відповідно до вимог стандарту ISO 27001.

3.5 Розробка пропозицій щодо оцінювання результативності й моніторингу системи забезпечення інформаційної безпеки

Аналіз ризиків може бути виконаний з різним ступенем деталізації в залежності від критичності ресурсів СУІБ / бізнес-процесів, відомих вразливостей і попередніх інцидентів інформаційної безпеки. Методологія оцінки ризиків може бути кількісною або якісною, або їх комбінацією. На практиці якісна оцінка часто використовується спочатку для визначення загального рівня ризику і визначення основних ризиків. Далі може виникнути необхідність виконання більш специфічного або кількісного аналізу стосовно основних ризиків. Кількісна оцінка ризиків є більш складною та потребує більше часу та ресурсів. Однак така оцінка буде дуже корисною у випадках, коли рішення щодо оброблення ризиків буде залежати від вартості заходів

безпеки, які можуть бути більшими, ніж фінансові втрати інциденту інформаційної безпеки.

Якісна методика оцінки ризиків використовує шкалу атрибутів для опису величини потенціальних наслідків реалізації загроз і вірогідність того, що такі наслідки виникнуть. Перевагою якісної методики є її простота розуміння всім персоналом; недоліком такої методики є залежність від суб'єктивного вибору шкали атрибутів.

Для отримання якісної оцінки ризиків необхідно розглянути оцінки наслідків реалізації загроз разом із вразливостями, з використанням яких ці загрози можуть реалізуватися, та оцінки ймовірності їх реалізації для кожного бізнес-процесу, мережі, обладнання, програмного забезпечення, які забезпечують функціонування цього бізнес-процесу, мережі університету в цілому, фізичного середовища, персоналу тощо.

Для виконання оцінки ризиків необхідно визначити шкалу для різних параметрів: оцінки величини наслідків реалізації загрози на сервіси безпеки (цілісність, конфіденційність, доступність, спостережність), оцінки ймовірності реалізації загрози. Загальний рівень оцінки величини наслідків реалізації кожної загрози на сервіси безпеки визначається як максимальна величина з окремих оцінок впливу на цілісність, конфіденційність, доступність, спостережність. Звертаємо увагу на те, що оцінка ймовірності не є математичною величиною вірогідності, яка не може перевищувати 1.

Рівень ризику за окремою парою загроза/вразливість, яка може використовуватися для реалізації цієї загрози, визначається перемноженням загального рівня оцінки величини наслідків на оцінку ймовірності реалізації загрози.

Загальний рівень ризику для бізнес-процесу, персоналу, фізичного середовища тощо дорівнює максимальної величині з усіх ризиків за кожною парою загроза/вразливість.

Рекомендуємо використовувати такі шкали для оцінки ризиків:

Для оцінки ймовірності реалізації загроз:

Таблиця 3.4

Оцінка ймовірності реалізації загроз

Оцінка ймовірності	Опис
1	Виникнення інциденту практично неможливо
2	Виникнення інциденту малоймовірне (не частіше ніж 1 раз на 1 рік)
3	Виникнення інциденту ймовірне до 1 разу на 3 місяці
4	Виникнення інциденту ймовірне до 1 разу на тиждень
5	Виникнення інциденту ймовірне до 1 разу на добу

Для величини наслідків реалізації загрози: вплив на цілісність:

Таблиця 3.5

Оцінка величини наслідків реалізації загрози на цілісність

Оцінка рівня наслідків	Опис
1	Практично не призводить до наслідків з фінансовими втратами
2	Призводить до незначних фінансових втрат (визначити суму) та має незначний вплив на репутацію Університету
3	Призводить до значних фінансових втрат (визначити суму) та має значний вплив на репутацію Університету
4	Призводить до великих фінансових втрат (визначити суму), має значний вплив на репутацію Університету і може призвести до зупинки роботи бізнес-процесу
5	Призводить до зупинки бізнес-процесу і порушує законодавство України

Для величини наслідків реалізації загрози: вплив на конфіденційність:

Таблиця 3.6

Оцінка величини наслідків реалізації загрози на конфіденційність

Оцінка рівня наслідків	Опис
1	Практично не призводить до розкриття конфіденційної інформації
2	Призводить до розкриття окремих документів, які відносяться до "комерційної таємниці", персональних даних і не призводить до фінансових втрат
3	Призводить до розкриття окремих документів, які

	відносяться до "комерційної таємниці", персональних даних і призводить до незначних фінансових втрат (визначити суму)
4	Призводить до розкриття документів, які відносяться до "комерційної таємниці", персональних даних і призводить до значних фінансових втрат (визначити суму), має значний вплив на репутацію Університету і може призвести до зупинки роботи бізнес-процесу
5	Призводить до зупинки бізнес-процесу і порушує законодавство України

Для величини наслідків реалізації загрози: вплив на доступність:

Таблиця 3.7

Оцінка величини наслідків реалізації загрози на доступність

Оцінка рівня наслідків	Опис
1	Практично не впливає на доступність
2	Вплив на доступність незначний (не більше 1/10 від максимально допустимого часу простою для цього бізнес-процесу)
3	Вплив на доступність середній (не більше - від максимально допустимого часу простою для цього бізнес-процесу)
4	Вплив на доступність значний (до максимально допустимого часу простою для цього бізнес-процесу)
5	Призводить до зупинки бізнес-процесу на тривалий час, який перевищує максимально допустимий час простою

Для величини наслідків реалізації загрози: вплив на спостережність:

Таблиця 3.8

Оцінка величини наслідків реалізації загрози на спостережність

Оцінка рівня наслідків	Опис
1	Практично не впливає
2	Вплив незначний
3	Призводить до неможливості відстежити частину дій виконавців бізнес-процесу
4	Призводить до неможливості відстежити дії виконавців і адміністраторів бізнес-процесу програмно-технічного комплексу

5	Призводить до неможливості відстежити дії виконавців і адміністраторів бізнес-процесу програмно-технічного комплексу, може призвести до зупинки бізнес-процесу, має вплив на репутацію Університету і порушує законодавство України

Визначення конкретних величин для параметрів оцінки повинно виконуватися з урахуванням досвіду працівників Університету, вимог нормативно-правових актів, історії попередніх інцидентів інформаційної безпеки, відомих випадків порушення інформаційної безпеки, досвіду інших фінансових установ тощо.

Рекомендуємо оцінку ризиків документувати у вигляді таблиці для кожного бізнес-процесу, приклад якої наданий у додатку 3.

Такий підхід до оцінки ризиків дозволить чітко виявити найбільші ризики у бізнес-процесах і найбільш критичні загрози.

Оброблення ризиків

Після виконання оцінки ризиків маємо оцінити альтернативні варіанти оброблення ризиків. Можливими варіантами оброблення ризиків можуть бути:

– зниження ризиків шляхом застосування належних заходів безпеки;

– свідоме та об'єктивне прийняття ризиків за умови, що вони чітко задовольняють політику організації та критерії прийняття ризиків;

– уникнення ризиків;

– перенесення відповідних бізнес-ризиків на інші сторони, наприклад, страхувальників, постачальників.

Для прийняття рішення щодо оброблення конкретних ризиків рекомендується визначити такі критерії стосовно кожного окремого ризику:

– низький ризик - 1 - 6;

– середній ризик - 7 - 14;

– високий ризик - 15 - 25.

Застосування належних заходів безпеки дозволить зменшити ризики. Під час вибору цих додаткових заходів безпеки повинні бути враховані всі вимоги законодавства України, нормативно-правових актів, внутрішніх документів, політики та стратегії Університету. Крім того, цей вибір також повинен враховувати вартість додаткових заходів безпеки, час їх впровадження, вплив на технологію операційної роботи, інтерфейс користувача тощо. З урахуванням цих факторів складається план оброблення ризиків. У разі необхідності тривалої підготовки до впровадження додаткових заходів безпеки деякі ризики можуть бути тимчасово прийняти як залишкові з включенням до наступного плану оброблення ризиків після перегляду оцінки ризиків.

Прийняття всіх залишкових ризиків повинно бути задокументовано і затверджено керівництвом Університету. Це стосується середніх та високих ризиків і повинно бути ретельно розглянуто. У документах стосовно прийняття залишкових ризиків має бути надана причина прийняття ризику та, за необхідністю, строки впровадження додаткових заходів безпеки для зниження ризику. Наприклад, якщо підприємством використовується програмно-технічний комплекс із застарілими технологіями, який має великий ризик реалізації однієї або декількох загроз і який планується замінити на новий більш сучасний комплекс протягом 2 років, то ці ризики можуть бути прийняти як тимчасове рішення до заміни цього програмно-технічного комплексу з наданням терміну впровадження нового.

Деякі ризики є властивістю існуючого бізнес-процесу / програмно-технічного комплексу. Особливу увагу слід звернути на вразливості саме програмно-технічних комплексів, які використовують застарілі або новітні незахищені технології. В деяких випадках слід розглянути питання щодо уникнення ризиків за рахунок зміни операційного середовища, баз даних, програмно-технічного комплексу, технології оброблення та зберігання інформації, оскільки це буде вимагати менших витрат, ніж впровадження додаткових заходів безпеки.

Висновки до розділу 3

Отже, в ході проведених досліджень ми встановили етапність проведення робіт з впровадження системи інформаційної безпеки в університеті та визначели алгоритм її формування.

ЗАГАЛЬНІ ВИСНОВКИ

На основі отриманого аналізу, ми відстежили порядок виконання дій та розмежували їх. За результатами проведеної роботи нами було визначено виконавців та осіб, що несуть відповідальність за функціонування кожного підрозділу та функції в ньому.

На основі цих даних нами було розроблено матрицю відповідальності з розмежуванням обов’язків кожного учасника процесу.

Разом з вищим керівництвом було визначено політику та цілі організації в системі забезпечення якісного управління та проведено роботи з документування у відповідні форми.

Також, ми розробили програму впровадження СУІБ. Програма складається з чотирьох етапів. Для кожного встановлено часові рамки виконання роботи. На основі цього прописано ймовірні результати, які мають бути отримані за результатами виконання програми з реалізації принципів СУІБ.

Можна зробити висновок, що вирішуючи ці проблеми, ми виконали роботу з:

– аналізу актуальності впровадження системи інформаційної безпеки в діяльність компанії;

– формування цілей і політики.

– виявлення та усунення зон безвідповідальності, або перехрещення відповідальності і розроблення матриці відповідальності для підприємства для успішного поетапного впровадження СУІБ.

– розроблення проекту впровадження системи інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ІНФОРМАЦІЇ

1. Офіційний сайт міжнародної організації зі стандартизації [Електронний ресурс] : – Режим доступу: https://www.iso.org/contents/news/2022/10/new-iso-iec-27001.html

2. Проблеми інформаційної безпеки вищої освіти в умовах глобалізації [Електронний ресурс] : – Режим доступу: https://er.knutd.edu.ua/bitstream/123456789/14498/1/PIONBUG_20191004_P125-126.pdf

3. Інформаційна безпека у навчальних закладах України [Електронний ресурс] : – Режим доступу: https://er.knutd.edu.ua/bitstream/123456789/10312/1/EOEMIR2018_P388-395.pdf

4. WEF: кібербезпека у 2022 році [Електронний ресурс] : – Режим доступу: https://10guards.com/ua/articles/wef-cybersecurity-2022/

5. Менеджмент інформаційної безпеки : опорн. консп. лекцій / уклад. І. З. Якименко. – Тернопіль : ТНЕУ, 2019. – 136 с.

6. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).

7. Стандарти ISO/IEC захистять від кіберзагроз. URL: http://csm.kiev.ua/ index.php?option=com_content& view=article&id=3631%3A-isoiec---&ca tid=122%3A2015-09-15-07-01-23&lang= uk.

8. ISO/IEC 27000. URL: http://pqm-online.com/ assets/files/pubs/translations/std/isomek-27000-2014.pdf.

9. Общие сведения о стандартах серии ISO 27000. URL: http://www.iso27000.ru/ standarty/iso-27000-mezhdunarodnyestandarty-upravleniya-informacionnoibezopasnostyu-1/iso-27000- mezhdunarodnye-standarty-upravleniyainformacionnoi-bezopasnostyu.

10. ISO/IEC 27000. URL: http://pqm-online.com/ assets/files/pubs/translations/std/isomek-27000-2014.pdf.

11. Керування механізмами захисту. Міжнародні стандарти інформаційної безпеки. URL: https://naurok.com.ua/keruvannyamehanizmami-zahistu-mizhnarodnistandarti-informaciyno-bezpeki-1047 26.html.

12. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT). URL: http://online.budstandart.com/ua/ catalog/doc-page.html?id_doc=66911.

13. ISO/IEC 27004:2009(E). URL: http:// www.klubok.net/Downloads-index-reqviewdownloaddetails-lid-425.html.

14. ISO/IEC 27005:2011(E). URL: http:// www.klubok.net/Downloads-index-reqviewdownloaddetails-lid-421.html.

15. Вашему бизнесу угрожают хакеры? Стандарт ISO/IEC 27031:2011 предлагает решения. URL: http://www.klubok.net/ article3.html.

16. ISO 27000 – группа стандартов по информационной безопасности. URL: http:// www.klubok.net/article2543.html.

17. Стандарти інформаційної безпеки: компаративне дослідження [Електронний ресурс] : – Режим доступу: http://pdu-journal.kpu.zp.ua/archive/2_2019/tom_1/16.pdf

18. Інтегрована система управління [Електронний ресурс] : – Режим доступу: https://nuph.edu.ua/sistema-upravlinnya-yakistyu-universit/

19. Стратегічний план розвитку НФаУ [Електронний ресурс] : – Режим доступу: https://nuph.edu.ua/wp-content/uploads/2019/06/%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%87%D0%BD%D0%B8%D0%B9-%D0%BF%D0%BB%D0%B0%D0%BD-%D1%80%D0%BE%D0%B7%D0%B2%D0%B8%D1%82%D0%BA%D1%83.pdf

20. Кавун С. В., Пилипенко А. А., Ріпка Д. О. Економічна та інформаційна безпека підприємств у системі консолідованої інформації. Навчальний посібник. Вид. ХНЕУ. 2013. 364 с. 61

21. Якименко Ю. М., Мужанова Т. М., Легомінова С. В. Системний аналіз технічних систем забезпечення інформаційної безпеки підприємств від компанії FIREEYE. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2020. № 4(12). С. 36-50.

22. Cheol Soon Park. A Study of Effect of Information Security Management System [ISMS] Certification on Organization Performance. [Electronic resource]. URL: http://paper.ijcsns. org/07_book/201003/20100303.pdf.

23. Calder A. Implementing Information Security based on ISO 27001/ISO 27002. A Management Guide. Van Haren, 2011. P. 90.

24. Гришко С., Кодрул Р. Інформаційна безпека підприємства та організація системи управління інформаційною безпекою: матеріали Всеукраїнської науково-практичної конференції, м. Харків, 1 листопада 2022 р. Харків, 2022 (подано до друку)

25. Маркіна І. А., Дячков Д. В. Основи формування системи менеджменту інформаційної безпеки підприємства. Проблеми і перспективи розвитку підприємництва. 2016. 3(1). 80 с.

26. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. КІІВіП НУ «ОЮА», 2017. 128 с.

27. Аспекти інформаційної безпеки в управлінні безперервністю діяльності організації http://its.iszzi.kpi.ua/article/view/190555/199051

28. Olechowski, A., Oehmen, J., Seering, W., and. Ben-Daya, M. 2016. The Professionalization of Risk Management: What Role Can the ISO 31000 Risk Management Principles Play?, Int. J. Proj. Manag. vol. 34, no. 8, стор. 1568–1578.

29. Kothari CR. Quantitative Techniques, 2nd ed., New Delhi: Vikas Publishing House Pvt. Ltd., 2009.

30. О.Є. Кузьмін, Н.Ю. Подольчак, Н.І. Подольчак, Л.Г. Вербицька. Управління ризиками в інноваційній діяльності: навч. посіб. Львів: Видавництво Львівської політехніки, 2012. 240 с.

ДОДАТКИ

ДОДАТОК А

ЖУРНАЛ
обліку інцидентів інформаційної безпеки
Національного фармацевтичного університету

Почато:
Закінчено:

1. Облік інцидентів, порушень та недоліків в роботі ІТ-інфраструктури

N з/п	Дата	Підрозділ, кафедра	Обставини інциденту, порушення, недоліків в роботі ІТ-інфраструктури	Учасники інциденту, порушення, недоліків в роботі ІТ-інфраструктури	Вжитті термінові заходи	Рішення керівника підрозділу/кафедри щодо вжиття першочергових заходів	Вжиті заходи щодо відновлення діяльності підрозділу/кафедри	Відмітка про виконання інструкцій з реагування
1	2	3	4	5	6	7	8	9

2. Зауваження осіб, які перевіряли обставини інциденту, порушення, недоліків в роботі ІТ- інфраструктури та вжиття відповідних заходів

_____

ДОДАТОК Б

НАЦІОНАЛЬНИЙ ФАРМАЦЕВТИЧНИЙ УНІВЕРСИТЕТ

ПОЛІТИКА

У СФЕРІ БЕЗПЕКИ ІНФОРМАЦІЇ

Місія НФаУ – розвиток національної галузі охорони здоров'я за рахунок здійснення всебічної підготовки компетентних фахівців на рівні стандартів Європейського простору вищої освіти. Разом з тим університет націлений на те, щоб забезпечити безпеку інформації особистої та корпоративної з ціллю покращення репутації та підвищення лояльності до Національного фармацевтичного університету

Для досягнення основної мети, ми використовуємо такі принципи:

- ***Надання освітніх послуг з можливістю онлайн навчання за графіком та на основі оптимальних інформаційних умов.***
- ***Досягнення задоволення зацікавлених сторін якістю наданих освітніх послуг.***
- ***Забезпечення високого рівня професійної підготовки персоналу та підвищення IT-обізнаності.***
- ***Оснащення сучасним, професійним обладнанням та застосування передових технологій для ефективного здійснення освітніх послуг.***
- ***Підвищення рівня безпеки персональних та корпоративних даних.***
- ***Оптимізація використання кадрових-, матеріальних- та фінансових-ресурсів для рішення завдань у сфері забезпечення безпеки інформації.***
- Ректор університету несе відповідальність за розробку, впровадження та функціонування системи забезпечення інформаційної безпеки відповідно до вимог міжнародних стандартів та постійне підвищення її результативності.
- Ця Політика є основою для роботи персоналу всіх структурних підрозділів/кафедр, реалізується системою забезпечення інформаційної безпеки і знаходиться під особистим контролем Ректора університету.
- Керівництво бере на себе відповідальність за реалізацію Політики у сфері безпеки інформації і зобов'язується забезпечити її розуміння та виконання всіма співробітниками університету.

ДОДАТОК В

НАЦІОНАЛЬНИЙ ФАРМАЦЕВТИЧНИЙ УНІВЕРСИТЕТ

ЦІЛІ

У СФЕРІ БЕЗПЕКИ ІНФОРМАЦІЇ

Вище керівництво виступає гарантом реалізації Політики у сфері безпеки інформації і бачить своє основне завдання в створенні умов праці, що забезпечують усвідомлене залучення працівників до процесу розробки, впровадження та актуалізації Системи забезпечення інформаційної безпеки і досягнення її цілей.

Вище керівництво визначає наступні шляхи досягнення Цілей у сфері безпеки інформації:

1. Розробити план та навчальні матеріали для тестування й підвищення кваліфікації співробітників у діючій системі забезпечення інформаційної безпеки компанії.
2. Впровадити систему ідентифікації матеріалів технічної та нормативної документації.
3. Уважно вивчити потреби, запити і очікування зацікавлених сторін на основі ефективного зворотного зв'язку розробити програму необхідних заходів.
4. В рамках розробленої програми надати зацікавленим сторонам вдосконалені комплексні пакети освітніх послуг.
5. Систематично підвищувати кваліфікацію і професійну підготовку персоналу 15 співробітників щорічно.
6. Провадити заохочуючі ініціативи та підвищувати відповідальність співробітників, спрямовану на поліпшення безпеки інформації, включити відповідні заходи до мотиваційної програми університету.

Кожен співробітник повинен особисто брати участь в досягненні поставлених цілей, розглядати здійснення освітньої послуги з точки зору забезпечення її інформаційної безпеки.

Національний фармацевтичний університет

Кафедра управління та забезпечення якості у фармації

ІІ Науково-практична internet-конференція з міжнародною участю
“Актуальні проблеми якості, менеджменту і економіки
у фармації і охороні здоров’я”

СЕРТИФІКАТ УЧАСНИКА № 55

Гончаров Станіслав

брав(ла) участь у роботі круглого столу “Інтеграція якості, лідерства та ефективності у менеджменті охорони здоров’я та фармації” за програмою обсягом
6 годин / 0,2 кредита ЄКТС
19 січня 2024 року, м. Харків

Досягнуті результати навчання:
використання у професійній діяльності знань щодо сучасних підходів менеджменту якості та управління соціально-економічними процесами в закладах охорони здоров'я та фармацевтичних організаціях, а також формування розвитку лідерських навичок у керівників

В.о. Ректора Національного фармацевтичного університету **Алла КОТВІЦЬКА**

МАТЕРІАЛИ

ІІ науково-практичної internet-конференції з міжнародною участю «АКТУАЛЬНІ ПРОБЛЕМИ ЯКОСТІ, МЕНЕДЖМЕНТУ І ЕКОНОМІКИ У ФАРМАЦІЇ І ОХОРОНІ ЗДОРОВ'Я»

(19 січня 2024 р.)

Міністерство охорони здоров'я України
Міністерство освіти і науки України
Національний фармацевтичний університет
Кафедра управління та забезпечення якості у фармації

МАТЕРІАЛИ

ІІ науково-практичної internet-конференції з міжнародною участю

«АКТУАЛЬНІ ПРОБЛЕМИ ЯКОСТІ, МЕНЕДЖМЕНТУ І ЕКОНОМІКИ У ФАРМАЦІЇ І ОХОРОНІ ЗДОРОВ'Я»

(19 січня 2024 р.)

MATERIALS

of II scientific and practical internet-conference
with international participation

«ACTUAL PROBLEMS OF QUALITY, MANAGEMENT, AND ECONOMY IN PHARMACY AND HEALTH CARE»

(19 January 2024)

Харків

2024

УДК 330.101:615.1

Реєстр з'їздів, конгресів, симпозіумів та науково-практичних конференцій: реєстраційне свідоцтво № 589 від 11.12.2023 р.

Актуальні проблеми якості, менеджменту і економіки у фармації і охороні здоров'я: матер. II міжнарод. наук.-практ. internet-конференції з міжнар. участю, Харків, 19 січня 2024 / ред. кол.: Т.В. Крутських, О.В. Посилкіна, О.В. Літвінова, Харків : НФаУ, 2024. – 515 с.

Actual problems of quality, management, and economy in pharmacy and health care: materials of II scientific and practical internet-conference with international participation. January 19, 2024 / ed. board. : T.V. Krutskikh, O.V. Posilkina, O.V. Litvinova, Kharkiv : NUPh, 2024. – 515 p.

Збірник містить матеріали II науково-практичної конференції, які присвячені обговоренню наукових та практичних проблем управління якістю і менеджменту в фармації і охороні здоров'я; визначенню напрямів удосконалення господарської й інноваційної діяльності підприємств (організацій, закладів) у ринковій економіці, підготовки сучасних кадрів із залученням вчених, фахівців-практиків, викладачів навчальних закладів та дослідників, докторантів, аспірантів, підприємців з України та зарубіжжя.

Матеріали подаються мовою оригіналу
За достовірність матеріалів відповідальність несуть автори

Гончаров С.В., Зборовська Т. В.

Національний фармацевтичний університет, м. Харків

Актуальність побудови інформаційної безпеки в діяльності організацій

t.v.zborovska@gmail.com

Вступ. Для України та всього світу 2023 рік видався важким у багатьох сенсах – зокрема й для глобальної кібербезпеки. Частота та винахідливість кібератак на бізнес, ланцюжки постачання та державні установи постійно зростає. За оцінками IBM, кожен витік даних наносить понад 4,3 млн доларів збитків й потребує щонайменше 200 днів на виявлення й ліквідацію наслідків. Постає питання як забезпечити безпеку у нестабільному цифровому світі? Це питання актуальне, не тільки для великого бізнесу з промисловим виробництвом, але й для навчальних закладів, оскільки вони містять багато інформації про особисті дані здобувачів та педагогічного персоналу. Щоб захиститися, потрібно розглядати умови виконання кроків захисту. Для їх розробки організації широко застосовують принципи та рекомендації, що містить стандарт ISO/IEC 27001.

Мета дослідження. За мету наших досліджень ми беремо визначення сучасних тенденцій щодо світової практики розробки схеми впровадження системи менеджменту інформаційної безпеки в організаціях.

Матеріали та методи. В досліджені ми використовуємо інформаційний метод дослідження літератури та Інтернет-ресурсів.

Отримані результати. Всесвітній економічний форум вніс кіберзлочинність до топ-10 найсерйозніших глобальних ризиків найближчого десятиліття. Свідчення тривожних тенденції можна представити наступним чином: за звітом SonicWall цього року загальна кількість кібератак зросла на 2% у порівнянні з 2022 роком – зафіксовано близько 5,5 млрд епізодів. Контролювати кіберзлочинність дуже важко. Експерти вважають, що глобально в поле зору правоохоронців потрапляють менш ніж 25% від усіх скоєних кіберзлочинів. Ступінь ризиків суттєво виросла через стійкий тренд на

віддалену працю та важке геополітичне середовище, де кібератаки стають важелем економічного і політичного впливу. У світі шириться принцип нульової довіри, який стає фундаментом безпеки у непередбачуваному цифровому середовищі. Його суть полягає в тому, що в організацій більше немає внутрішнього периметра, який можна вважати безпечним. Кожен користувач, кожен процес і кожен пристрій у системі мають ретельно перевірятися. Права доступу до даних слід обмежувати настільки, наскільки це можливо. Тому навчальні заклади також мають його дотримуватися.

На основі проведених досліджень ми пропонуємо універсальну схему реагування на кіберзагрози в першу чергу вірусні атаки в організації (Рис.1).

Рис. 1. Схема реагування на кіберзагрози.

Висновки. Сучасний кіберпростір не можна назвати безпечним місцем, тому ідея нульової довіри актуальна як ніколи. Адже сьогодні корпоративні диджитал-екосистеми виходять далеко за межі власної мережі, охоплюючи віддалену (дистанційну) роботу, партнерські організації та пристрої безконтактного Інтернет зв'язку. Однак використання сучасних технологій та безпекових практик допомагає мінімізувати ризики.

Ф А 2.2.1–25-366

Національний фармацевтичний університет

Факультет фармацевтичних технологій та менеджменту
Кафедра управління та забезпечення якості у фармації
Рівень вищої освіти другий магістерський
Спеціальність 073 Менеджмент
Освітня програма Якість, стандартизація та сертифікація

ЗАТВЕРДЖУЮ
Завідувачка кафедри
управління та забезпечення
якості у фармації
Тетяна КРУТСЬКИХ
“17” жовтня 2023 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

Станіслава ГОНЧАРОВА

1. Тема кваліфікаційної роботи: **"Розробка пропозицій щодо впровадження системи менеджменту інформаційної безпеки на прикладі діяльності навчальних закладів"**, керівник кваліфікаційної роботи: Тетяна ЗБОРОВСЬКА, канд. фармац. наук, доцент,

затверджений наказом НФаУ від “16”жовтня 2023 року № 229

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи: 05.02.2024 р.

3. Вихідні дані до кваліфікаційної роботи: наукова та навчально-методична література, законодавчі й нормативні акти України, вимоги стандарту ISO/IEC 27001.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
Актуальність роботи. Мінімізація можливості виникнення інформаційних ризиків, підприємства потребує впровадження ефективних системи управління інформаційною безпекою. Ці системи повинні включати в себе заходи щодо запобігання, виявлення та реагування на інформаційні ризики.
Розділ І. Інформаційна безпека в управлінні діяльностю сучасної організації. Роль та місце інформаційної безпеки в інформаційному суспільстві. Стан кібербезпеки та заходи у сфері інформаційної безпеки. Джерела загроз та засоби їх впливу на об’єкти інформаційної безпеки. Етапи розвитку нормативної бази у сфері інформаційної безпеки. Розроблені стандарти інформаційної безпеки для захисту підприємств.
Розділ ІІ. Аналіз діяльності підприємства. Складові інформаційної безпеки підприємства. Інтегрована система управління якістю навчального закладу.
Розділ ІІІ. Практичні підходи до формування системи інформаційного захисту університету. Організація кроків впровадження системи інформаційного управління університету. Розробка політики та цілей системи інформаційної безпеки. Етапи ідентифікації інформаційних активів. Розробка програми впровадження СУІБ в діяльність університету. Розроб-

ка пропозицій щодо оцінювання результативності й моніторингу системи забезпечення інформаційної безпеки.

Висновки. Для формування алгоритму інформаційної безпеки нами запропоновано впровадити в діяльність оцінку інформаційних ризиків, облік активів для захисту та розподілити відповідні повноваження між співробітниками.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень):

1. Журнал записів інцидентів.
2. Політика у сфері безпеки інформації
3. Цілі у сфері безпеки інформації

6. Консультанти розділів кваліфікаційної роботи

Розділ	**Ім'я, ПРІЗВИЩЕ, посада консультанта**	**Підпис, дата**	
		завдання видав	**завдання прийняв**
Вступ	Тетяна ЗБОРОВСЬКА, доцент закладу вищої освіти кафедри управління та забезпечення якості у фармації		
Розділ І	Тетяна ЗБОРОВСЬКА, доцент закладу вищої освіти кафедри управління та забезпечення якості у фармації		
Розділ ІІ	Тетяна ЗБОРОВСЬКА, доцент закладу вищої освіти кафедри управління та забезпечення якості у фармації		
Розділ ІІІ	Тетяна ЗБОРОВСЬКА, доцент закладу вищої освіти кафедри управління та забезпечення якості у фармації		
Висновки	Тетяна ЗБОРОВСЬКА, доцент закладу вищої освіти кафедри управління та забезпечення якості у фармації		

7. Дата видачі завдання: 17.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Термін виконання етапів кваліфікаційної роботи	Примітка
1.	Формулювання мети, задач, об’єкту та предмету досліджень в рамках кваліфікаційної роботи	17.10.2023 р.	**виконано**
2.	Складання розширеного плану та опрацювання етапів виконання кваліфікаційної роботи	18.10.2023 р.	**виконано**
3.	Збір літературних джерел та проведення загального літературного огляду за напрямком теми	19.10.2023 р.	**виконано**
4.	Обґрунтування актуальності обраного напрямку досліджень, зведення статистичних даних	24.10.2023 р.	**виконано**
5.	Складання та оформлення вступу до кваліфікаційної роботи	26.10.2023 р.	**виконано**
6.	Складання та оформлення І-го розділу роботи (літературний огляд, теоретичні засади)	31.10.2023 р.	**виконано**
7.	Проведення аналізу об’єкту та предмету досліджень, аналіз ситуації на базі стажування	07.11.2023 р.	**виконано**
8.	Оформлення ІІ-го розділу роботи (аналітична частина) з формулюванням проблематики	21.11.2023 р.	**виконано**
9.	Розробка прикладних пропозицій для розв’язання визначених у ІІ-му розділі проблем	28.11.2023 р.	**виконано**
10.	Оформлення ІІІ-го розділу роботи з обґрунтуванням раціональності висунутих пропозицій	15.12.2023 р.	**виконано**
11.	Оформлення додатків до роботи (розроблених документів та форм, запропонованих заходів)	21.12.2023 р.	**виконано**
12.	Остаточне оформлення кваліфікаційної роботи та пред’явлення її для перевірки керівником	08.01.2024 р.	**виконано**
13.	Розробка мультимедійних слайдів та складання плану доповіді. Робота з рецензентами.	15.01.2024 р.	**виконано**
14.	Проходження попереднього захисту, коригування роботи, підготовка до офіційного захисту	19.01.2024 р.	**виконано**

Здобувач вищої освіти _____ Станіслав ГОНЧАРОВ

Керівник кваліфікаційної роботи _____ Тетяна ЗБОРОВСЬКА

ВИТЯГ З НАКАЗУ № 229
по Національному фармацевтичному університету
від 16 жовтня 2023 року

Про затвердження тем кваліфікаційних робіт

Затвердити теми кваліфікаційних робіт, керівників-консультантів та рецензентів здобувачам вищої освіти **2 курсу,** спеціальність – **073 Менеджмент**, освітня програма – **Якість, стандартизація та сертифікація**, ступінь вищої освіти – **магістр**, термін навчання – **1 р. 6 міс.**, очна (**денна**) та **заочна** форми здобуття освіти.

Прізвище, ім'я по батькові здобувача вищої освіти	Тема кваліфікаційної роботи (українською мовою)	Тема кваліфікаційної роботи (англійською мовою)	Керівник кваліфікаційної роботи	Рецензент кваліфікаційної роботи
Гончаров Станіслав Віталійович	Розробка пропозицій щодо впровадження системи менеджменту інформаційної безпеки на прикладі діяльності навчальних закладів	Development of proposals for the implementation of the information security management system based on the example of the activities of educational institutions	к.фарм.н., доцент, доцент ЗВО кафедри управління та забезпечення якості у фармації, Зборовська Т. В.	к.фарм.н., доцент, доцент кафедри технологій фармацевтичних препаратів НФаУ Пуляєв Д. С.

В.о. ректора **Алла КОТВІЦЬКА**

Вірно:
Декан факультету фармацевтичних технологій та менеджменту **Наталія ЖИВОРА**

Ф А2.8-47-110

ВИСНОВОК

Комісії з академічної доброчесності про проведену експертизу

щодо академічного плагіату у кваліфікаційній роботі

здобувача вищої освіти

№ 126315 від « 9 » лютого 2024 р.

Проаналізувавши випускну кваліфікаційну роботу за магістерським рівнем здобувача вищої освіти денної форми навчання Гончарова Станіслава Віталійовича, 2 курсу, _____ групи, спеціальності 073 Менеджмент , на тему: «Розробка пропозицій щодо впровадження системи менеджменту інформаційної безпеки на прикладі діяльності навчальних закладів / Development of proposals for the implementation of the information security management system based on the example of the activities of educational institutions», Комісія з академічної доброчесності дійшла висновку, що робота, представлена до Екзаменаційної комісії для захисту, виконана самостійно і не містить елементів академічного плагіату (компіляції).

Голова комісії,
професор **Інна ВЛАДИМИРОВА**

6%
8%

Ф А 2.2.1-32-353

ВІДГУК

наукового керівника на кваліфікаційну роботу другого (магістерського) ступеня вищої освіти спеціальності 073 Менеджмент освітньої програми Якість, стандартизація та сертифікація

Станіслава ГОНЧАРОВА

на тему "Розробка пропозицій щодо впровадження системи менеджменту інформаційної безпеки на прикладі діяльності навчальних закладів"

Актуальність теми. Міжнародна організація зі стандартизації в ISO 27001 встановлює вимоги до системи управління інформаційної безпеки для демонстрації здатності організації захищати свої інформаційні ресурси. Метою такої системи є вибір відповідних заходів управління безпекою, призначених для захисту інформаційних активів і гарантій довіри зацікавлених сторін. Ця система впроваджується, щоб забезпечити основу для побудови організаційної стійкості до інформаційних ризиків, що дозволить організації функціонувати, таким чином, що б захищати бізнес, репутацію та інтереси всіх зацікавлених сторін.

Практична цінність висновків, рекомендацій та їх обґрунтованість. Проаналізовані у роботі дані літературних джерел і досвід впровадження дали автору підставу розглянути характеристику університету та процеси управління в межах існуючої системи інформаційного захисту та провести огляд кроків для впровадження СУІБ. В результаті виконання роботи було проведено дослідження специфіки впровадження СУІБ та розроблено програму, яка складається з чотирьох етапів та націлена на виконання покрокової реалізації плану інформаційного захисту університету.

Оцінка роботи. У процесі виконання кваліфікаційної роботи здобувач опанував навички роботи з науковою літературою, навчився збирати, систематизувати, аналізувати, узагальнювати інформацію, закріпив набуті протягом навчання теоретичні знання та практичні навички. Кваліфікаційна робота належно оформлена і написана лаконічною науковою мовою, містить необхідні структурні елементи та посилання на актуальні джерела літератури.

Загальний висновок та рекомендації про допуск до захисту. Враховуючи вищенаведене, вважаю, що робота здобувача 2-го курсу спеціальності 073 Менеджмент освітньої програми Якість, стандартизація та сертифікація Станіслава ГОНЧАРОВА на тему "Розробка пропозицій щодо впровадження системи менеджменту інформаційної безпеки на прикладі діяльності навчальних закладів" за обсягом та змістом відповідає вимогам, що висуваються до кваліфікаційних робіт вищих навчальних закладів IV рівня акредитації і може бути представлена до захисту в Екзаменаційну комісію Національного фармацевтичного університету.

Науковий керівник
доцент закладу вищої освіти кафедри управління
та забезпечення якості у фармації
канд. фармац. наук, доц. _____ Тетяна ЗБОРОВСЬКА
“16” січня 2024 року

Ф А2.2.1-32-356

РЕЦЕНЗІЯ

на кваліфікаційну роботу здобувача другого (магістерського) ступеня вищої освіти спеціальності 073 Менеджмент освітньої програми Якість, стандартизація та сертифікація

Станіслава ГОНЧАРОВА

на тему "Розробка пропозицій щодо впровадження системи менеджменту інформаційної безпеки на прикладі діяльності навчальних закладів"

Актуальність теми. Сучасні методи обробки, передачі та накопичення інформації сприяли появі загроз, пов'язаних з можливістю втрати, перекручування та розкриття даних, які адресовані або належать кінцевим користувачам. Тому забезпечення інформаційної безпеки комп'ютерних систем і мереж є одним з провідних напрямків розвитку ІТ. Комп'ютерні інформаційні технології швидко розвиваються та вносять помітні зміни в наше життя. Інформація стала товаром, який можна придбати, продати, обміняти. При цьому вартість інформації часто в сотні разів перевершує вартість комп'ютерної системи, в якій вона зберігається. Нині перед суб’єктами діяльності гостро стоїть питання щодо вирішення спільної проблеми – інформаційної безпеки.

Теоретичний рівень роботи. Аналіз літературних джерел дав розуміння ситуації щодо питання інформаційної безпеки, аналіз проведений автором, довів доцільність впровадження системи захисту та визначив порядок відповідних дій з боку суб’єкта господарювання.

Пропозиції автора з теми дослідження. Виходячи з актуальності питання, основною метою роботи Станіслава ГОНЧАРОВА стала розробка заходів з впровадження системи інформаційної безпеки задля збереження конфіденційності, цілісності й доступності обігу інформації в ЗВО. Автор кваліфікаційної роботи пропонує певні кроки здійснення інформаційного захисту.

Практична цінність висновків, рекомендацій та їх обґрунтованість. Результатами даної роботи є встановлення підходів до визначення наявних та необхідних ресурсів впровадження системи інформаційної безпеки. Також здобувачем було представлено програму системи управління інформаційної безпеки університету та сформовано методичні підходи до її впровадження.

Недоліки роботи. У роботі є зауваження до оформлення окремих літературних посилань та рекомендується більш детально провести роботи з розподілення повноважень некерівного складу працівників університету, але це не впливає на зміст та значущість, а також на загальне позитивне враження від роботи.

Загальний висновок і оцінка роботи. Кваліфікаційна робота належно оформлена і написана лаконічною науковою мовою, містить необхідні структурні елементи та посилання на джерела літератури.

Враховуючи вищенаведене, вважаю, що робота здобувача 2-го курсу спеціальності 073 Менеджмент освітньої програми Якість, стандартизація та сертифікація Станіслава ГОНЧАРОВА на тему "Розробка пропозицій щодо впровадження системи менеджменту інформаційної безпеки на прикладі діяльності навчальних закладів" за обсягом та змістом відповідає вимогам, що висуваються до випускових робіт вищих навчальних закладів IV рівня акредитації і може бути представлена до захисту в Екзаменаційну комісію Національного фармацевтичного університету.

Рецензент
доцент кафедри технологій
фармацевтичних препаратів НФаУ
канд. фарм. наук, доцент, _____Денис ПУЛЯЄВ
“25” січня 2024 року

ВИТЯГ З ПРОТОКОЛУ № 6
засідання кафедри управління за забезпечення якості у фармації НФаУ

від «19» січня 2024 р.

ГОЛОВУЮЧИЙ: д.фарм.н., проф. Крутських Т.В.
СЕКРЕТАР: к.фарм.н., доц. Лісна А.Г.
ПРИСУТНІ: зав. каф., проф. Крутських Т.В., проф. Коваленко С.М., проф. Посилкіна О.В., проф. Літвінова О.В., проф. Братішко Ю.С., доц. Баєва О.І., доц. Гладкова О.В., доц. Глєбова Н.В., доц. Деренська Я.М., доц. Зборовська Т.В., доц. Коляда Т.А., доц. Ковальова В.І., доц. Лісна А.Г., доц. Ткаченко О.В., доц. Мороз С.Г., здобувач вищої освіти Гончаров С.В.

ПОРЯДОК ДЕННИЙ:

1. Попередній захист кваліфікаційної роботи здобувача вищої освіти спеціальності 073 Менеджмент, освітньої програми Якість, стандартизація та сертифікація другого (магістерського) рівня Станіслава ГОНЧАРОВА на тему «Розробка пропозицій щодо впровадження системи менеджменту інформаційної безпеки на прикладі діяльності навчальних закладів».

СЛУХАЛИ: доповідь до кваліфікаційної роботи здобувача вищої освіти спеціальності 073 Менеджмент, освітньої програми Якість, стандартизація та сертифікація другого (магістерського) рівня Станіслава ГОНЧАРОВА на тему «Розробка пропозицій щодо впровадження системи менеджменту інформаційної безпеки на прикладі діяльності навчальних закладів».

УХВАЛИЛИ: допустити Станіслава ГОНЧАРОВА до захисту кваліфікаційної роботи на засіданні Екзаменаційної комісії.

Зав. кафедри управління та забезпечення якості у фармації, професор _____ **Тетяна КРУТСЬКИХ**

Секретар кафедри _____ **Анастасія ЛІСНА**

Ф А2.2.1-32-042

НАЦІОНАЛЬНИЙ ФАРМАЦЕВТИЧНИЙ УНІВЕРСИТЕТ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Направляється здобувач вищої освіти Станіслав ГОНЧАРОВ до захисту кваліфікаційної роботи
за галуззю знань 07 Управління та адміністрування
спеціальністю 073 Менеджмент
освітньою програмою Якість, стандартизація та сертифікація
на тему: "Розробка пропозицій щодо впровадження системи менеджменту інформаційної безпеки на прикладі діяльності навчальних закладів"

Кваліфікаційна робота і рецензія додаються.

Декан факультету _____ / Наталія ЖИВОРА

Висновок керівника кваліфікаційної роботи

Здобувач вищої освіти Станіслав ГОНЧАРОВ підготував кваліфікаційну роботу, яка відповідає всім вимогам, виконана у встановлені строки, має наукову новизну та може бути рекомендована до захисту.

Керівник кваліфікаційної роботи Тетяна ЗБОРОВСЬКА

_____

“18” січня 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційну роботу розглянуто. Здобувач вищої освіти Станіслав ГОНЧАРОВ допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувачка кафедри
Управління та забезпечення якості у фармації

_____ Тетяна КРУТСЬКИХ

“19” січня 2024 року

Кваліфікаційну роботу захищено

у Екзаменаційній комісії

13 лютого 2024 року

З оцінкою _____

Голова Екзаменаційної комісії:

доктор наук з державного управління, кандидат економічних наук, професор, заслужений діяч науки і техніки України
професор кафедри публічного управління та підприємництва Національний аерокосмічний університет імені М.Є. Жуковського "Харківський авіаційний інститут"
Андрій ДЄГТЯР

_____
(підпис)